WEB AND MOBILE BASED EXAMINATION RESULTS DISSEMINATION AND VERIFICATION SYSTEM USING AUTHENTICATED ENCRYPTION – A CASE OF TECHNICAL EDUCATION VOCATIONAL AND ENTREPRENEURSHIP TRAINING AUTHORITY

by

Lister Mseteka

A Dissertation submitted to the University of Zambia in partial fulfilment of the requirements for the award of the degree in Masters of Engineering in Information Communication Technology Security

The University of Zambia
School of Engineering

LUSAKA

2019

DECLARATION

I, the undersigned, declare that the work in this dissertation is original except where otherwise indicated by references and has not previously been submitted for any degree or academic qualification. A complete list of references is appended.

Name: Mseteka Lister Signature:…….Date:…….

Supervisor: Dr. Jackson Phiri Signature:…….Date:……..

APPROVAL

This document by Lister Mseteka is approved as fulfilling the requirements for the award of the degree of Masters of Engineering in Information and Communication Technology Security of the University of Zambia.

Examiner 1:…….Signature:……Date:……

Examiner 2:…….Signature:……Date:……....

Examiner 3:…….....Signature:……Date:……..

Chairperson:…….....Signature:……Date:…….
Board of
Examiners

Supervisor: Dr. Jackson Phiri Signature:…….Date:…….

ACKNOWLEDGEMENT

I give praise and thanks to God the father of our Lord Jesus Christ for the guidance throughout the course of this study. I am grateful to Dr. Jackson Phiri and Dr. Simon Tembo for guiding me throughout the research process, may the God almighty bless you all. I would also like to thank staff in TEVETA registered institutions, IT staff at TEVETA and students in TEVETA registered institutions for responding favourably to the questionnaires. I would also like to thank my family for the love and support they gave me throughout my studies.

DEDICATION

To my family and friends. Thank you all for the love, encouragement and support. I am extremely grateful to Dr. Jackson Phiri who helped enormously and guided me with his knowledge and experience throughout my research to completion.

ABBREVIATIONS

AES	Advanced Encryption Standard
CIA	Confidentiality, Integrity and Availability
DES	Data Encryption Standard
3DES	Triple Data Encryption Standard
DFA	Differential Fault Analysis
ECTA	Electronic Communications Transaction Act
ECZ	Examinations Council of Zambia
ERD	Entity Relationship Diagram
HMAC	Hashed Message Authentication Code
HTML	Hyper Text Mark Up Language
ICT	Information and Communication Technology
MANEB	Malawi National Examinations Board
MD2	Message Digest 2
MD4	Message Digest 4
MD5	Message digest 5
NIST	National Institute of Standards and Technology
OOD	Object Oriented Design
PHP	Hypertext Preprocessor
QR	Quick Response
UML	Unified Modelling Language
USSD	Unstructured Supplementary Service Data
RSA	Rivest-Shamir-Adleman
SDLC	System Development Life Cycle
SHA	Secure Hash Algorithm
SMS	Short Messaging Service
SSL	Secure Socket Layer
TEVETA	Technical Education Vocational and Entrepreneurship Training Authority

TEVET	Technical Education, Vocational and Entrepreneurship Training
ZICTA	Zambia Information and Communication Technology Authority

ABSTRACT

Institutions of higher learning retain sensitive data making them highly attractive targets for cybercrime. However, most developing countries and public higher institutions of learning have low levels of Information and Communication Technology (ICT) and hence face challenges in securing information and information systems. Therefore, the dissemination of students' examination results by public higher institutions through web and mobile applications usually raise security concerns on how to ensure the confidentiality, integrity and authenticity of students' examination results due to susceptibility of web and mobile applications to cyber attacks. In this study, a model was designed for secure storage and dissemination of students' examination results using encryption and cryptographic hash functions to provide information security objectives of confidentiality, integrity and authenticity assurances on students' examination results. The study was guided by three (3) objectives. A baseline study was conducted to determine the challenges faced by Zambia's Technical Education, Vocational and Entrepreneurship Training Authority (TEVETA) and students regarding dissemination of students' examination results in order to address objective number one (1). The results from the study indicate that the current TEVETA business processes have a number of irregularities. These include candidate registration, storage of students' examination results and dissemination of students' examination results. The results from the baseline study were used to design a model which was then used to develop the prototype in order to address the second (2) and third (3) objective. The results obtained from the test and evaluation of the developed prototype based on the model showed not only improved efficiency in dissemination of examination results but also confidentiality of students' results through encryption as well of integrity of students' examination results through detection of altered students' examination results during transmission and storage through cryptographic hash function.

Keywords – encryption, Examination Dissemination system, integrity, Hash function.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE
INTRODUCTION

1.1 Introduction

Most developing countries and public higher institutions of learning have low levels of Information and Communication Technology (ICT) and hence face challenges in securing information and information systems. The conventional method of storing student examination results on paper or insecure electronic records is often characterised with high fraudulent practices ranging from fake results, falsification of results due to unauthorised amendments to results and unauthorised disclosure. Currently, educational institutions have become heavily reliant on ICT for delivering educational services such as, examination results, study schedules, lectures and other information institutions wish to communicate to stakeholders [11]. There has been a recent increase in the use of web and mobile applications in educational institutions for dissemination of students' examination results [12]-[16]. However, the dissemination of examination results through web and mobile applications has raised security concerns on how to ensure the confidentiality, integrity and authenticity of students' examination results. This is because web and mobile applications are susceptible to cyber attacks which can compromise the confidentiality, integrity and authenticity of data [17] - [19].

Technical Education, Vocational and Entrepreneurship Training Authority (TEVETA) is an institution in Zambia created under the Technical Education, Vocational and Entrepreneurship Training Act (No. 13 of 1998) read together with TEVET (Amendment) Act No. 11 of 2005. Its purpose among others is to regulate and conduct national examinations related to technical education and award certificates to persons who succeed in examinations. TEVETA conducted its first national examinations in 2010 [20]. It has a total of 304 registered institutions country wide [20] and a total of 25,650 students as at 31st December 2016 [21]. As at 31st December 2016, TEVETA

developed, reviewed and approved a total of 247 curricula at diploma, advanced certificate, certificate, trade test and skill award levels. Out of the 247 revised curricula, 53 were at diploma level, 22 advanced certificate, 57 certificate, 89 trade test and 41 at skills awards [20], [21]. There has been an increase in the number of candidates sitting for examinations from a total of 10,493 in 2010 to 25,650 in 2016 representing an increase of 41 percent [20]. The increase in the number of candidates sitting for examinations has put a heavy strain on the examination body and has led to challenges in the release of examination results on time.

In this study, a web and mobile prototype for efficient dissemination of TEVETA examination results was developed. Further, the prototype aimed to improve the confidentiality and integrity of examination results using encryption and cryptographic hash functions.

1.2 Motivation of the Research

The enormous impact of erroneous student examination results due to wrongly computed results [23]- [25] and loss of data integrity due to cyber attacks [16] demands meticulous student result computation, secure storage and secure transmission of results respectively. An evaluation of studies related at improving the security of web and mobile based Information Systems for dissemination of students' examination was worth undertaking as it helped come up with measures to help address security challenges in the current web and mobile examination results dissemination information systems. This study propose secure transmission and storage of students' examination results using encryption and cryptographic hash functions in order to provide information security objectives of confidentiality, integrity and authenticity assurances on examination results.

1.3 Scope

This research involved a baseline study that was conducted in three (3) provinces of Zambia, seven (7) districts and twelve (12) institutions of study to establish the challenges

faced by TEVETA and students regarding dissemination of examination results. The results obtained from the baseline study indicate that the current TEVETA business processes for candidate registration and dissemination of examination results has a number of irregularities. These irregularities include candidate registration, storage, dissemination and how students access the results. The business processes identified formed the basis of the developed web and mobile prototype for dissemination of results. The web and mobile USSD application require hosting with an Internet Service Provider and a gateway to send and receive requests to and from the mobile service provider respectively. Hosting a web site and subscribing to mobile service providers was expensive to the researcher. A local web server was used to host a web application and a USSD simulator was developed for a mobile application.

1.4 Problem Statement

TEVETA face a challenge in dissemination of students' examination results. Currently, TEVETA produce nominal rolls and statements of results that are sent to institutions of study where students check their results from. This method of results dissemination takes long to be accomplished and as a result examination results are always delayed. The delay in the release of students' examination results consequently result in reduction of the first term of the TEVET academic calendar from three (3) months to a month as students are not allowed to proceed to the next level of study before examination results are released. Further, the current method of storing students' examination results in plain text in the database without encryption gives room for possibility of unauthorised results disclosure, results modification and identity theft. It is against this background that this study attempted to address the questions in section 1.7.

1.5 Aim

The aim of this study was to design and implement a web and mobile based examination results dissemination system using encryption and cryptographic hash functions in order to enhance the confidentiality, integrity and authenticity of examination results.

1.6 Research Objectives

The research objectives that constituted this study were:

1. To conduct a baseline study to establish the challenges faced by TEVETA and students regarding dissemination of students' examination results.
2. To design a model based on TEVETA business processes and ISO 27001 information security standard in order to address challenges in (1).
3. To develop a secure web and mobile prototype for storage and dissemination of examination results based on the model in (ii).

1.7 Research Questions

The following questions were addressed to meet the above objectives:

1. What are the challenges faced by TEVETA and students regarding dissemination of students' examination results?
2. Is it possible to design a model based on current TEVETA business processes and ISO 27001 information security standard to address challenges in (1)?
3. How can a secure web and mobile prototype for storage and disseminate examination results be developed?

1.8 Significance of the Study

The study provides secure storage and dissemination of students' examination results using encryption and cryptographic hash functions to provide information security objectives of confidentiality, integrity and authenticity assurances on students' examination results.

1.9 Organisation of the Dissertation

This dissertation is divided into five (5) chapters. Chapter 1 is the introduction to the research. It discusses the background to the study, problem statement, aim and

motivation of this thesis. Chapter 2 looks at literature review and related works. Chapter 3 looks at the methodology that was used in this research. The methods used to ascertain the challenges faced by TEVETA and students regarding dissemination of examination results and statistical information are outlined. Chapter 4 outlines the presentation of the findings of the baseline study, system implementation and testing. Chapter 5 discusses the findings of the research and conclusion, also stating future works and recommendations.

1.10 Summary

This chapter focused on introduction to the research, motivation of the research, scope, problem statement, aim, research objectives, research questions, research contribution and organisation of the thesis

CHAPTER TWO
LITERATURE REVIEW

2.1 Introduction

In this chapter, the literature and works related to this research study is given. Firstly, an extensive review of literature on information security risks and information security challenges faced by examination bodies and tertiary institutions in securing student information is given. This is followed by a brief review of Advanced Encryption Standard algorithm and SHA3-224 cryptographic hash function technologies and how they can be used to improve the security of examination results. This chapter closes by looking at related works where mobile or web applications have been used for dissemination of examination results.

2.1.1 Theoretical Framework

Information is the most coveted commodity in the information age. In the academic sector, information is especially important. Educational institutions (e.g. examination bodies, Universities, Polytechnics and Colleges) are expected to manage and preserve student information. The information includes bio data, personal identification information such as student identification code, picture or other information that identify a student, special education needs, disciplinary records, medical records, courses undertaken, documentation of attendance, qualifications earned, grades and transcripts. If students' information is not properly created, processed and stored, it can cause errors [23] - [25]. Errors in student information may lead to delayed release of students' examination results as institutions spend more time correcting erroneous records [26], [27] and sometimes with wrong grades calculated [25], [28]. Further, the traditional method of storing student examination results in plain text without encryption gives room for possibility of unauthorised results disclosure, results modification and identity theft.

A 2017 Data Breach Investigations Report by Verizon reveals that there were 455 cybersecurity incidents in the educational sector and that 73 of them resulted in data breaches [29]. The integrity of students' academic records is crucial as fraudulent results impact on public confidence in the credibility of examination authorities (examination bodies and tertiary institutions).

2.2 Information Security threats in Higher Education Institutions

Security risks on information systems in higher learning institutions are not theoretical, as some incidents have revealed. A 2017 Data Breach Investigations Report by Verizon reveals that there were 455 cybersecurity incidents in the educational sector and that 73 of them resulted in data breaches [29]. In this section, a review of security threats faced by higher learning institutions is outlined.

2.2.1 Global Perspective

Perlroth [30] highlighted that 53 Universities, including Harvard, Stanford, Cornell Princeton, Johns Hopkins, the University of Zurich and other Universities around the world were hacked in 2011. The hacking resulted in publication of 36,000 email addresses, thousands of names, usernames, passwords, addresses and phone numbers of students, faculty and staff to web site named Pastebin.com. A 2017 report by Verizon [29] indicate that 455 cyber security incidents in the education sector occurred and that 74 of them resulted in data breaches. The British Broadcasting Corporation (BBC) in 2018 reported that the University of Greenwich in the United Kingdom was fined £120,000 ($160,000) by the Information Commissioner as fine for a security breach in which 19,500 students' records were placed online [31]. The data included names, addresses, dates of birth, phone numbers, signatures and - in some – cases – physical and mental health problems.

2.2.2 Regional Perspective

In Kenya, the Catholic University of Eastern Africa faced security breaches, where students hacked into the system and altered grades, registered for courses they had not covered yet and graded them, cleared/altered their financial balances [32]. According to the Cyberoams's report released during the education Cyber Security Symposium, Kenyan students are fourth in Africa after Egypt, Morocco and South Africa in terms of hacking school systems to manipulate grades and fees [33]. In 2011, a report from the Office of the Permanent Secretary, Ministry of Higher Education, Science and Technology was circulated to all Vice Chancellors of public Universities and Principals of University Colleges in Kenya about a group of University students that compromised academic and financial systems' integrity by altering grades and fee balances in favour of others [34]. The affected Universities were Jomo Kenyatta University of Agriculture and Technology, the Catholic University of Eastern Africa, Daystar University and Maseno University. In another incident, employees and students of Kenyatta University hacked into the university's database and altered examination results [35].

Mugyenyi [36] noted that a number of incidences that occurred at Makerere University in Uganda in which student marks were altered, fees defaulters sneaking on the graduation lists and poor management of students' payment details among others was due to poor information system security.

2.3 Security Challenges in Higher Education Institutions

An open and diverse environment is a standard requirement in higher education [37], [38]. Under most circumstances, higher education institutions are strapped for resources to manage the equilibrium between openness and security against malware and sensitive data exfiltration. Generally, security professionals need to strike a

balance between adding security barriers to prevent an attack and allowing a system to remain functional for users [39]. As security increases, the system functionality and ease of use decreases for users. Figure 1 shows the security, ease of use and functionality triangle.

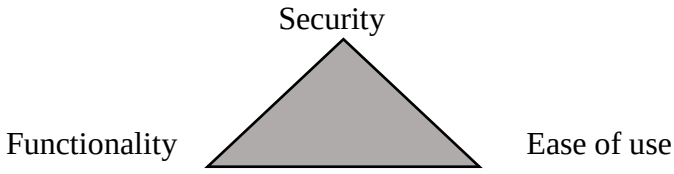


Fig. 1: Security, functionality and ease of use triangle. Source; [39].

A SANS survey in 2014 on 300 higher education IT professionals confirm difficulties in making their environments secure while also providing openness institutions need for their students, staff, parents and benefactors [37]. Higher education institutions are prime targets of cybercrime because of the following reasons:

- Wide variety of valuable data

Institutions of higher learning retain sensitive data about students personal records, students accounting system, students grade information, student medical records, staff records, payroll information, faculty information, research data, and other sensitive information institutions may store making them highly attractive targets for cybercrime [29], [49].

- Widespread use of personal devices

The widespread use of various less well-protected mobile devices coupled with lack of security awareness by students, administrators and staff when accessing sensitive data leads to exposure of sensitive data making institutions of higher learning easy targets for hackers [40], [41].

- Lack of centralised structure

Institutions store sensitive data in different locations rather than on a centralised location and the same data may kept in other locations: school, department and central administration. The decentralised structure gives cybercriminals a wide range of paths to exploit vulnerabilities in the disjoint systems that store sensitive data [38], [40]. In

addition, the responsibility for implementing security measure may lie with different stakeholders in a wide range of departments, making it difficult for Information Technology (IT) security personnel to enforce information security on all schools, departments, staff and students [38], [40].

Given the importance of the information stored in higher education institutions, it is imperative that information security should be an important managerial concern. For a higher education institution where large amounts of student information is hosted on administrative systems and Learning Management Systems, any information leakage or loss would have large impacts [42]. Information security protects information assets from unauthorised access, disclosure, modification and destruction to ensure its confidentiality, integrity and availability [22], [39], [43]. Information security is the assurance of the conventional CIA (confidentiality, integrity and availability) triad of information security [22], [39] and a plethora of other security related concepts and principles of identification, authentication, authorisation, privacy, auditing, non-repudiation and accountability [39].

2.4 Security Awareness and Training in Higher Education Institutions

Higher education institutions are prime targets of cybercrime because they retain highly sensitive data such as students personal records, students accounting system, students grade information, student medical records, staff records, payroll information, faculty information, research data etc. Although there are many technical solutions to help protect the information assets of an organisation, there can be no security that can be trusted without a security policy. A security policy is a document(s) that summarises the security requirements of an organisation and prescribes the steps necessary to achieve the desired security. An organisation's security policy provides the first or innermost layer of defence for its information assets and without a security policy there can be no security that can be trusted [46], [47], [82].

Another crucial ingredient in information security apart from the security policy and technical solutions is user awareness and training. No matter how good a job IT professionals do to tighten security on organisation's networks and systems, they have to deal with the weakest link – the users [44]. This is the reason why Information security governance, compliance and awareness have become emerging issues in higher education institutions.

2.4.1 Global Perspective

A study by Nasser [48] in Yemen focussed on information security governance in public Universities. The result of the findings show that management's participation level is inadequate to deal effectively with information security governance threats, and that roles and responsibilities are not well defined in support of information security governance practices.

Chan and Mubarak [49] conducted a study to investigate and assess information security weakness levels within South Australian Higher Education Institutions. The study revealed that information security awareness levels were lacking and recommended information security awareness as part of overall risk assessment strategies in order to mitigate risks.

Marks and Rezgui in Malaysia conducted a research and found out that factors such as conscientiousness, cultural assumptions and beliefs, and social conditions affect University staff behaviour and attitude towards information security awareness [50]. In another study in Malaysia, Hina and Dominic [51] argue that information security policy compliance in higher education institutions remains scare, as is the realisation of security threats and dissemination of information security policies to end users. Still in Malaysia, the research finding by Muniandy et al. [52] show that the current state of cyber security behaviour among higher education students in the aspects of: password usage, phishing, social engineering, online scam and malware was generally unsatisfactory. The researchers strongly recommended that cyber security education

be implemented as part of the higher education curriculum because students are not given the opportunity to learn and understand the evolving cyber security threats.
Eyadat conducted a research to investigate the importance of information security program in 59 higher education institutes in the United States [53]. The findings indicated lack of support and supervision by top management for information security program. Furthermore, Eyadat [53] noted an alarming high rate of unawareness of security with no education and training programs available in the surveyed institutes.

Al-Alawi et al. [54] evaluated the levels of knowledge, attitude, and behaviour of the end-users regarding information systems security awareness at Kuwait University. The study revealed poor levels of information systems security awareness among end users.

According to Bruijn and Janssen [55] in Netherlands, cyber security is a complex and multifaceted area that require evidence based message framing. They argue that the inability to frame cyber security has resulted in failure by governments and citizens to take appropriate measures and develop suitable policies. The authors recommends that cybersecurity specialists, researchers and policy-makers need to communicate cyber security awareness clearly to avoid misunderstanding and ambiguity.

2.4.2 Regional Perspective

A study by Magomelo et al. [56] focused on identification and evaluation of information security governance practices that were implemented in Zimbabwean Universities. The findings from the research provided evidence that although management and the University Council understand the importance of information security, no acceptable code of best practice was implemented. The study recommended that management and University Councils should provide support to information security governance which includes risk management, strategic alignment and resource management.

Chandarman and Nierkerk [57] conducted a study to assess levels of computer security awareness at a tertiary education institution in South Africa. The findings revealed poor computer security awareness and hence recommended the need for targeted computer security awareness campaigns to users.

Mugyenyi [36] noted that although the Ugandan government has operationalised cyber laws and the National ICT policy, most higher learning institutions are still threatened by cyber attacks such as alteration of student marks, fees defaulters sneaking on the graduation lists and poor management of students' payment details among others. He recommended that much emphasis should be put in developing suitable cyber security models that are able to work hand in hand with the implemented policies of the institutions to achieve the institutions' goals in a cost effective manner.

Antwi-Bekoe and Nimako [58] conducted a study to assess computer security awareness and computer security vulnerabilities based on user practices among computer users in two public Universities in Ghana. The study revealed that different levels of computer security awareness and computer security vulnerabilities exist among three subgroups namely faculty staff, administrative staff and students. The authors recommended that there is need to enforce compliance to organisational policies. Still in Ghana, a research by Adu and Adjei [54] underscores that cyber security awareness and policies within corporate organisations in Ghana is low and that most organisations are not integrating legal aspects into their information security policies.

In Kenya, a study by Okibo and Ochibe [60] established that the challenges facing information systems security management in higher learning institutions are system vulnerability, computer crime and abuse, environmental security and financial backing/security. The study recommended implementation of new policies and procedures to guide information system security. Ndiege and Okello [61] investigated

information security awareness amongst undergraduate students at a higher education institution in Kenya. The findings from the study indicate that the majority of the students did not possess adequate understanding of information security awareness. It was recommended that information security awareness be incorporated in the undergraduate curriculum to help enhance awareness.

In conclusion, there can be no effective security without an organisation security policy, security awareness and training. Therefore, higher education institutions must ensure that employees receive training in information security awareness in order to implement what is in the organisation security policy.

2.5 CYBER LAW

Besides security policies, user awareness and training, there is need for cyber laws to criminalise perpetrators of cybercrime. Cybercrimes cannot be addressed by traditional laws because traditional laws were not written with technology in mind. However, many countries now have laws, regulations and policies governing information security, such as the Data protection Act, Computer Misuse Act of the United Kingdom and the Federal Information Security Management Act in the United States [42]. Zambia too has operationalised cyber laws, including the Computer Misuse Act (2004), The Information and Communications Technology Act (2009), Electronic Communication and Transactions Act (2009) and the National ICT Policy of 2007 [62], [63]. Simusokwe [64] noted that the enactment of the Zambia National ICT policy of 2007 shows government's commitment towards promoting security in the ICT sector as cyber security concerns have been addressed and several guides for future legislative reforms identified.

Zambia like any other country in the world is vulnerable to cyber attacks. The operationalisation of cyber laws and the National ICT Policy by the Zambian government is an indication of commitment towards safeguarding information and IT infrastructure for government, public and private organisations, and individual

privacy from cyber attacks. Therefore, the design of a secure web and mobile based examination results dissemination system for TEVETA using encryption and cryptographic hash function is important to curb cyber attacks that can compromise the integrity, authenticity and integrity of students' examination results.

2.6 Security Standards

Besides laws, policies and regulations governing information security, many national and international standards for Information Security Management have been established. The standards help to ensure that all relevant elements of security are addressed in an organisation's security strategy. The most widely adopted standard is the ISO 27001 Information Security Management System [65]-[69]. It is an internationally recognised structured methodology that specifies requirements for establishing, implementing and documenting information security management systems. ISO 27001 has a total of 39 control objectives and 134 measures for security management. Organisations should ensure that they cover the full range of controls needed to protect the confidentiality, integrity and availability of business information from various threats [70]. The control objectives are listed in table 1, subdivided by domains. The domains are security policy, organisation of information security, asset management, human resources, physical and environment security, communication and operation management, access control, information security incident management, business continuity management and compliance.

Table 1 ISO 27001 control objectives [71].

Domain	Control Objectives
Security Policy	To provide managerial direction and support for information security in accordance with business requirements and relevant laws and regulations
Organisation of Information Security	To manage information security within the organisation. To maintain the security of the organisation's

	information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
Asset management	To achieve and maintain appropriate protection of organizational assets. To ensure that information receives an appropriate level of protection.
Human resources security	To ensure that employees, contractors, and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error. To ensure that all employees, contractors and third party users exit an organisation or change employment in an orderly manner.
Physical and environmental security	To prevent unauthorised physical access, damage and interference to organisation's premises and information. To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.
Communications and Operations managements	To ensure the correct and secure operation of information processing facilities. To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements. To minimize the risk of system failures. To protect the integrity of software and software To maintain the integrity and availability of information and information processing facilities. To maintain security of information and software exchanged within an organisation and with external entities. To ensure the security of electronic commerce services, and their secure use. To detect unauthorised information processing activities.
Access Control	To control access to information. To ensure authorised user access and to prevent unauthorised access to information. To prevent unauthorised user access, compromise or theft of information and information processing facilities. To prevent unauthorised access to networked services. To prevent unauthorised access to operating systems.

	To prevent unauthorised access to information held in operating systems To ensure information security when using mobile computing and teleworking facilities.
Information systems acquisition, development and maintenance	To ensure that security is an integral part of information systems. To prevent errors, loss, unauthorised modification or misuse of information in applications. To protect the confidentiality, authenticity or integrity of information by cryptographic means. To ensure security of system files. To maintain the security of application system software and information. To reduce risks resulting from exploitation of published technical vulnerabilities.
Information security incident management	To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. To ensure a consistent and effective approach is applied to the management of information security incidents.
Business continuity management	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
Compliance	To avoid breaches of any law, statutory, regulatory, or contractual obligations, and of any security requirements. To ensure compliance of systems with organizational security policies and standards. To maximize the effectiveness of and to minimize interference to/from the information systems.

In this study, the model is based on TEVETA business processes, information systems acquisition, development and maintenance and access control domains of the ISO 27001 standard [71].

2.7 Review of the Literature

2.7.1 Technologies

In this study, two technologies will be looked at; Advanced Encryption Standard (AES) and Secure Hash Algorithm 256 (SHA256) for securing students' results during storage and transmission.

2.7.1.1 Need for Network Security

The desire to share resources within and outside the organisation has led to the increase in the use of computer networks and the internet. In addition, most businesses and governments use mobile phones, computer networks and internet for communication across the internet. The increase in electronic communication across the insecure network (Internet) has led to an increase in cyber related security issues. Security attacks now take the form of eavesdropping, masquerading, message tempering and denial of service among others. There is a pervasive need for measures to guarantee the confidentiality, integrity and availability of resources in computer systems.

2.7.1.2 Cryptography

Cryptography provides security to data during processing, transmission and storage. Scientists and mathematicians have developed a series of complex algorithms to ensure confidentiality, integrity, authentication and nonrepudiation or accountability of data during processing, transmission and storage. On the other hand, hackers and governments spent time undermining the algorithms. Cryptography has been around for some time and are all based upon an algorithm which is a set of mathematical rules that dictates how encryption and decryption processes should take place. Encryption is the art and science of hiding the meaning or intent of the message from

unintended recipients [39]. Modern cryptography utilize complex algorithms and long cryptographic keys to achieve information security objectives of confidentiality, integrity, authentication and non-repudiation. There are three types of cryptographic algorithms commonly used today; symmetric encryption algorithms, asymmetric encryption, and hashing algorithm.

(a) Symmetric Key Algorithms

Symmetric key algorithms rely on a shared secret key that is distributed to all members who participate in the communication for encryption and decryption of messages. Figure 2 shows the symmetric algorithm for encrypting and decrypting messages.

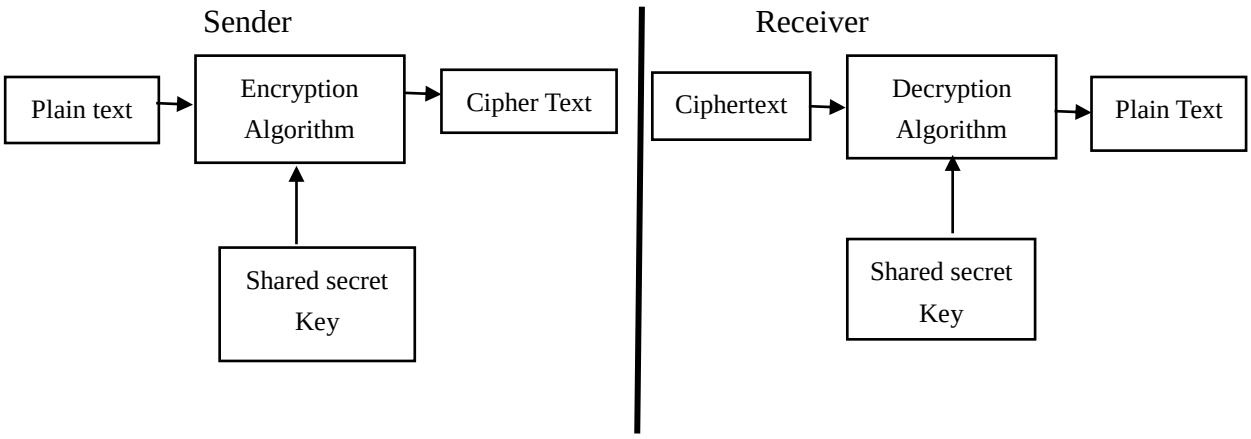


Fig. 2: Symmetric Key Cryptography

Popular examples of symmetric key cryptosystems are: the Data Encryption Standard (DES), Triple DES (3DES), International Data Encryption Standard (IDEA), Blowfish, Skipjack, and the Advanced Encryption Standard (AES). The major advantage of symmetric key cryptography is the great speed at which it encrypts and decrypts messages, often 1,000 to 10,000 times faster than asymmetric [39]. However, symmetric key Cryptography has the following weaknesses:

(i) Key distribution: Parties must exchange the secret key securely before establishing communications. The security of a symmetric algorithm rests in the key;

disclosing the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secret, the key must remain secret.

(ii) Repudiation: Any communication party can encrypt and decrypt the message with the shared secret key, there is no way to tell where the message came from

(iii) Keys are regenerated often: Old keys must be discarded every time a participant leaves the group.

(b) Asymmetric Key Algorithms

Asymmetric algorithms (also called Public-key algorithms) are designed so that the key used for encryption is different from the key used for decryption. The algorithms are called "public-key" because the encryption key can be made public: A complete stranger can use the encryption key to encrypt a message, but only a specific person with the corresponding decryption key can decrypt the message. In these systems, the encryption key is often called the public key, and the decryption key is often called the private key. The three common public key cryptosystems in use today are: Rivest-Shamir-Adleman (RSA), El Gamal and Elliptic Curve Cryptosystem.

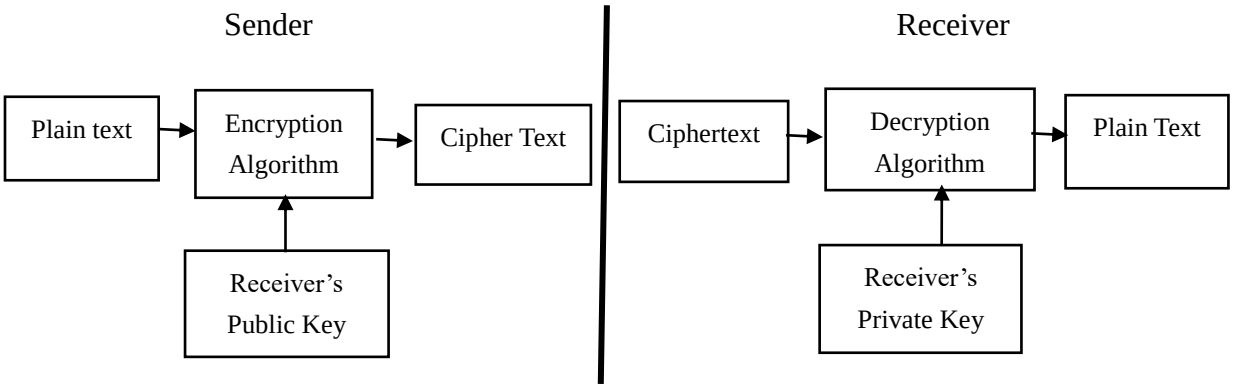


Fig. 3: Asymmetric Key Cryptography

The following are the major strengths of asymmetric key cryptography:

i. Key regeneration required only when a private key is compromised

If a key is compromised or a user leaves a community, the systems administrator only needs to invalidate that user's keys. No other keys are compromised and therefore key regeneration is not required for other user.

ii. Key distribution is simple: Users who want to participate in the system make their public keys available to anyone who may want to communicate with them

iii. Keys can be removed easily from asymmetric systems: Asymmetric key algorithms provide revocation mechanism that allows keys to be cancelled, removing a user from the system

iv. No pre-existing communication link required: Two parties can communicate securely without a preexisting relationship. All that both parties need to do is publish their public keys.

v. Integrity, authentication and non-repudiation: If a user does not share their private key, any message signed can only be accurately verified by a corresponding published public key.

The major weakness of public key cryptography is its slow speed operation. Because of this reason, many applications that require secure transmission of large amounts of data use public key to establish a connection and then exchange a symmetric secret key and encryption and decryption of data is through symmetric encryption algorithm [39], [72]. The comparison between symmetric and asymmetric cryptography are in table 2.

Table 2 Comparison of Symmetric and Asymmetric Cryptography

Symmetric	**Asymmetric**
Single shared key	Key pair sets
Out-of-band exchange	In-band exchange
Not scalable	Scalable
Fast	Slow
Bulk encryption	Small block of data, digital signatures, digital envelopes, digital certificates
Confidentiality	Integrity, authenticity, non-repudiation

Source: [39]

A practically secure cryptosystem does not exist because there are always theoretically known attacks that any cryptosystem may be exposed to. Practical

security describes an abstract idea that cannot be achieved in totality in real world. However, if cryptosystem attacks require unrealistic resources in 'reasonable' operational time for any attacker, then it is practically secure. There are a number of characteristics of practically secure cryptosystems:

(1) **Computational Complexity**.

Computational complexity is concerned with the time taken to conduct an attack. A very basic design principle for determining practical security should ensure that no known attack on the cryptosystem can be conducted in less than the cover time of the plaintext. The cover time is the length of time for which a plaintext must be kept secret. A well-designed cryptosystem is usually built around a computational problem that is widely perceived to be hard to solve. If a given encryption algorithm is known to be difficult to solve and may have a number of solutions, the hacker would have a surmountable task to solve it. Therefore, secured encryption can be examined within the scope of computational complexity to determine whether a solution exists in polynomial time [22], [73]. Therefore, all that the users of an encryption algorithm can strive for is an algorithm that meets one or both of the following criteria [22], [73]:

i. The cost of breaking the cipher exceeds the value of the encrypted information.
ii. The time required to break the cipher exceeds the useful lifetime of the information.

An encryption scheme is said to be computationally secure if either of the foregoing two criteria are met. Unfortunately, it is very difficult to estimate the amount of effort required to cryptanalyse ciphertext successfully.

(2) **Key Management.**

Most effective attacks on cryptosystems exploit bad key management practices [22], [73]. Therefore, it is important to keep the shared key and private key secret in symmetric key cryptography and asymmetric key cryptography respectively.

(c) Hashing Algorithms

Hashing algorithms are used to produce message digests, hash value or a finger print of a message, such that, it is extremely difficult, if not impossible, to derive a message

from an ideal hash function, and very unlikely that two messages will produce the same message digest, hash value or fingerprint. A cryptographic hash function must satisfy the following three criteria:

1. Preimage Resistance

Given a message m and the hash function hash, if the hash value h = hash (m) is given, it should be hard to find any m such that:

$$h = \text{hash}(m) \qquad \text{Equation (1)}$$

2. Second Preimage Resistance (Weak Collision Resistance)

Given input m 1, it should be hard to find another message m 2 such that hash (m 1) = hash (m 2) and that:

$$m\,1 \neq m\,2 \qquad \text{Equation (2)}$$

3. Strong Collision Resistance

It ought to be hard to find two messages $m\,1 \neq m\,2$ such that:

$$\text{hash}(m\,1) = \text{hash}(m\,2). \qquad \text{Equation (3)}$$

The following are the common hashing algorithms in use today:

- Message Digest 2 (MD2)
- Message Digest 4 (MD4)
- Message Digest 5 (MD5)
- Secure Hash Algorithm (SHA)
- Hashed Message Authentication Code (HMAC)

MD2, MD4 and MD5 Hashing Algorithms

Message digest MD2, MD4, and MD5 were designed by Ronald Rivest. However, MD2, MD4 and MD5 algorithms are no longer accepted as suitable hashing functions [39]. Several mathematicians have published articles documenting flaws in these algorithms.

Secure Hash Algorithm (SHA)

Secure Hash Algorithm (SHA) was developed by National Institute of Standards and Technology (NIST) and published as Federal Processing Standard (FIPS 180) in 1993

[74]. Recent cryptanalytic attacks demonstrated that there are weaknesses in the SHA-1 algorithm that led to the creation of SHA-2, which has four variants: SHA-224, SHA-256, SHA-384, and SHA-512 [31]. A 2011 cryptanalytic attack breaks pre-image resistance for 57 and 80 rounds of SHA-512, and 52 out of 64 rounds for SHA-256 [75]. 256 SHA-256 and SHA-512 are also prone to length extension attacks; by guessing the hidden part of the state, length attacks on SHA-224 and SHA-384 are possible. SHA-3 is the latest member of SHA released by NIST in 2015 [37], [76], [77]. The SHA-3 family consists of SHA3-224, SHA3-256, SHA3-384, and SHA3-512, and two extendable-output functions (XOFs), called SHAKE128 and SHAKE256.

Hashed Message Authentication Code (HMAC)

The Hashed Message Authentication Code (HMAC) algorithm guarantees the integrity of the message during transmission but does not provide non-repudiation. HMAC can utilise any SHA-2 variants in conjunction with a shared secret key. Therefore, the only communication parties who know the key can verify the message digest or digital signature. If the recipient decrypts the message but cannot successfully compare it to a message digest generated from the plain-text message, then the message was altered in transit.

2.8 Proposed Technologies for Secure Web and Mobile Examination Results Dissemination

As earlier mentioned in this paper, Public Key Cryptography is very slow and cannot be used to encrypt bulk messages like in the case of students' examination results [39], [72]. Therefore, AES, a symmetric algorithm was used for encryption and decryption of students' marks and SHA3- 224 algorithm for verifying the integrity of stored encrypted marks. During storage, not only are encrypted marks stored in the

database but also a hash of plaint text marks, for the purpose of verifying the integrity of students' marks before displaying examination results. If the integrity of the marks is compromised, the application stops compromised examination results from being displayed. Section 2.8.1 and Section 2.8.2 gives justification on why AES algorithm and SHA3-224 hash algorithms were used in a Web and Mobile Based Examination Results Dissemination and Verification System for TEVETA for providing confidentiality, integrity and authenticity assurances on students' examination results.

2.8.1 The Advanced Encryption Standard (AES)

The United States government published DES in 1977 as a proposed standard cryptosystem for all government communication [39]. In 2000, NIST announced that DES had been replaced by AES. In that same year, United States mandated encrypting all sensitive but unclassified data using AES [77]. It is noted by Boxcryptor [78] that AES is most widely used and secure encryption algorithm used in banks, governments and high security systems around the world.

Mahan and Sachdeva [79] measured the performance of three (3) encryption algorithms namely; AES, DES and RSA algorithms. Based on the text files and the experimental results, it was concluded that AES algorithm consumes least encryption time compared to RSA. It was also observed that decryption using AES algorithm is better that other algorithms. From the simulation results, it was established that AES is better than DES and RSA algorithm. Mushtaque [80] analysed various symmetric key encryption algorithms such as DES, 3DES, Blowfish, CAST-128, MARS, IDEA, AES and RC6 based on different parameters such as: architecture, scalability, security, flexibility, and limitations. After the comparison, it was concluded that AES is secure, fast, better and effective among all the encryption algorithms and has least memory usage, high encryption performance, without any weakness and limitations while other algorithms have some weakness and differences in performance and storage space [80]. Afolabi and Atanda [81] analysed four popular and commonly used encryption algorithms: RSA, DES, 3DES and AES based on the encryption time,

memory usage, output byte, power consumption rate, flexibility and security. Experimental results from the study show that AES consumes least encryption time and has least memory usage. The results also showed that while there is a minor difference in encryption time between AES and DES, RSA consumes large encryption time and that memory usage is very high. It was concluded that AES was the best among all the encryption algorithms in terms of security, flexibility, memory usage, encryption performance, and power consumption rate [81]. Singhal and Singhal [46] compared AES and RSA algorithms. The results of the study show that encryption and decryption takes more time in RSA algorithm than AES. Hercigonja et al. [72] provided an analytical study on various symmetric encryption algorithms such as DES, 3DES, CAST-128, AES, RC6 and asymmetric RSA algorithm based on architecture of algorithms, security and limitations they have. The results showed that although asymmetric algorithms are superior in security than all symmetric algorithms, they take more time to encrypt or decrypt information and use more memory. In symmetric encryption, results showed that RC6, Blowfish and AES are more secure and efficient in terms of processing and memory usage.

Therefore, AES algorithm was used for encryption and decryption of students' marks or grades as it has been established by many researchers as the most secure and efficient algorithm among symmetric algorithms and more efficient than the popular asymmetric encryption algorithm such as RSA.

2.8.2 SHA3- 224 Hashing Algorithm

Luo *et al*. [45] proposed an efficient and powerful method to conquer the SHA-3 family of hash algorithms using Differential Fault Analysis (DFA). The findings from the study show that DFA on SHA3-224 and SHA3-256 are more difficult than on SHA3-384 and SHA3-512, while SHA3-224 is more difficult to conquer than SHA3-256. Therefore, SHA3-224 will be used to hash marks to provide integrity checks before displaying examination results.

Therefore, SHA3-224 was used for hashing encrypted marks to provide integrity

checks before decrypting examination results for each student.

2.9 Related Works

There has been an increase in the number educational institutions disseminating examination results through mobile and web applications [12], [14] - [16]. Although educational institutions benefit from using web and mobile applications for dissemination of examination results, web and mobile applications are susceptible to cyber attacks [17] - [19] which can compromise the confidentiality, integrity and authenticity of academic records. The protection of students' academic records such as grades, financial records, medical records, attendance records, bio data or even biometric data is important yet difficult undertaking.

Web applications are subject to cyber attacks due to inherent security vulnerabilities and insecure software development life cycle [18], [83]. It has been noted by Kaur and Kaur [83] that secure coding is not easy because of today's competitive era of getting applications online to meet deadlines, hence security is not given the required importance during web application development.

Mobile application are subject to cyber attacks such as SMS spamming, message disclosures, denial of service (DOS) and SMS phishing. A research by Mirzoev *et al.* [84] reveal that many mobile devices have inherent security vulnerabilities and are not equipped with standard security software. Therefore, they are vulnerable to malicious programs, theft of information and performance degradation (denial of service attack). It was noted by Mirzoev *et al.* [84] that many mobile applications are rushed through development and deployed without security requirements during application development.

The challenge of securing students records has further been propounded by adoption of cloud computing for storage of voluminous data in higher educational institutions. Several recent studies have recommended the adoption of cloud computing in higher education institutions to curb problems of high cost of storage [9], [85] - [91].

However, storage of information in the cloud often raise concerns on security, location of data, legal jurisdictions, reliability of the service provider, privacy and regulatory compliance [92].

Various studies have been conducted aimed at improving the security of web and mobile information systems for dissemination of examination results. The study by Adagunodo *et al*. [12] presented a Short Message Service (SMS) application that enables University students to access both current and old examination results by sending an SMS along with a password [12]. However, the SMS propagates between the sender and the receiver in unencrypted form, hence susceptible to cyber attacks. Further, examination results were stored in plain text without encryption hence vulnerable to cyber attacks. Olusanya and Ogaba [93] developed a system 'Results Alert through SMS and Email' that enables students to access examination results through email and SMS. However, results were transmitted and stored in the database in plain text without encryption, hence can be viewed or modified by anyone who has access to the database. Muhamadi *et al.* [14] developed an 'Auto Notification Service for the Student Record Retrieval System Using Short Message Service (SMS)' that automatically sends an SMS to each student once a Lecturer submits a mark to their records. However, the main emphasis on security is user and administrative access to the database [14].

In order to eliminate the high cost of software acquisition/licenses, maintenance, infrastructure, support and security treats of vendor results computation systems on the market, Ise [11] proposed a result computation system as a cloud service to eliminate the aforementioned costs. In addition, the author proposed securing computed results data using AES algorithm during transmission and before storage of examination results. However, encryption is not enough for securing students' marks as there is a possibility that an insider or hacker without the knowledge of the key may hack into the database and swap encrypted marks from one student record in the database to another in preference of a particular candidate. Since symmetric algorithms use the same key

for encryption and decryption, the swapped encrypted marks decrypt correctly when a user sends a request to view results. In an effort to reduce delays in processing and release of examination results in tertiary institutions, Obinyi and Ezugwu [94] developed an enhanced computer program that speeds up collection of processed results from various departments over a network to a centralised database. However, results were stored in plain text in the database making them vulnerable to unauthorised disclosure and modification. Ibrahim [13] developed an application that enables students to access academic services such as assessment performance, study schedules and institution's provision of information to students irrespective of their geographic location [13]. The security incorporated is a one-time password in the SMS. However, the study by Ibrahim [13] only addressed security issues in the SMS but examination results were stored in plain text without encryption.

Rantiola *et al.* [95] developed a mobile application that allows students to use an SMS to access examination results. The application provides a secure means of accessing examination results using multifactor authentication. Multifactor authentication only proved the true identity of the user before granting access to examination results. However, examination results were stored in plain text in the database without encryption and hence vulnerable to cyber attacks.

Mukarukundo [96] designed and implemented a mobile application for efficient dissemination of examination results. However, the SMS propagates between the mobile phone and the SMS gateway in unencrypted form, hence susceptible to cyber attacks. In addition, examination results were stored in plain text in the database, giving room for possibility of unauthorised results disclosure and results modification.

Zabangwa [15] designed and implemented an SMS results dissemination system for Examinations Council of Zambia (ECZ) that enables pupils to access examination results as soon as they are available using a mobile phone. However, examination results were stored in plain text in the database without encryption.

Solomon and Phiri [27] proposed a Short Message Service/Unstructured Supplementary Service Data (SMS/USSD) mobile application using cloud technologies to enhance candidate registration for examinations and dissemination of examination results for Malawi National Examinations Board (MANEB). The main emphasis on security is on administrative and user access to the database. However, examination results in the database were stored in plain text without encryption.

Mshangi *et al.* [16] proposed a secure web and mobile-based information system for dissemination of students' examination results using Soft Science Design Methodology (SSDM) that embrace secure coding practices, security awareness training and education [16]. Mshangi *et al.* in their study recommended encryption of the communication channel for both SMS and web traffic. However, encryption of the SMS communication channel or web traffic only provides confidentiality of examinations results during transmission but results were stored in plain text in the database and hence vulnerable to cyber attacks.

Joshi et al. [97], designed and implemented a Results Alert System through Email and SMS. The main objective was to surmount the challenges that most higher learning institutions face in making examination results and grades accessible to students. However, examination results were stored in plain text without encryption.

Mseteka and Phiri [98], proposed a secure model for storage and dissemination of examination results using encryption and cryptographic hash function. The results from the study show that the model provides confidentiality of examination results through encryption and integrity of examination results through detection of altered results during storage or transmission through cryptographic functions. In another study, Mseteka et al [99], proposed a secure web and mobile application for dissemination of examination results dissemination system using encryption and cryptographic hash for secure storage and dissemination of examination results. The results from the study show that the developed prototype provides an avenue for confidentiality of results

through encryption and detection of altered results (thus providing integrity and authenticity assurances of results) through cryptographic hash function.

2.10 Summary

In this chapter, a comprehensive background of the need for information security in higher education institutions, threats, challenges and some examples of related works aimed at securing students' academic records were given.

CHAPTER THREE
METHODOLOGY

3.1 Introduction

This chapter describes the research methods and materials that were employed in this research.

3.2 Baseline Study

A baseline study was conducted to determine the challenges faced by TEVETA and students regarding dissemination of students' examination results. A mixed research methods (quantitative and qualitative research methods) were used in this study to explore the challenges faced by TEVETA and institutions regarding dissemination of examination results. The use of different research methods enables deeper understanding of the problem at hand [100]. For quantitative data, questionnaires were administered to a total of 558 respondents consisting of 8 TEVETA ICT staff, 514 students and 36 members of staff in-charge of TEVETA examinations from 12 TEVETA registered institutions of study in Zambia. For Qualitative data, interviews were conducted with some ICT staff at TEVETA.

3.2.1 Study Population

The target population were TEVETA examination candidates, members of staff from institutions of study responsible for candidate registration for examinations and TEVETA ICT staff responsible for candidate registration, examinations results entry and managing Information Systems.

3.2.2 Sample Size and Sampling Procedure

The study population was purposively sampled. Non-probability sampling technique was used for all respondents to facilitate inclusion of the best candidates based on the role of the respondents. This approach was preferred as the research required information from TEVETA examination candidates, TEVETA ICT members of staff responsible for candidate registration for examination results and examination results entry. Further, the research required information from members of staff from institutions of study who register candidates for TEVETA examinations. Data was collected from 558 respondents consisting of five hundred and fourteen (514) students, thirty six (36) members of staff in-charge of examinations from institutions of study and eight (8) TEVETA IT staff.

The formula that was used for calculating the sample size from the student study population is as follows:

$$n = \frac{N}{1 + (e)^2} \qquad \text{Equation (4)}$$

where n is the sample size , N is the population size, and e is the level of precision or accuracy, normally set at 0.05 [101], [102]. TEVETA had a total of 25,650 students in 2016 [21].

$$n = \frac{25650}{1 + (0.05)^2}$$

$$n = \frac{25650}{1 + 64.125}$$

$$n = \frac{25650}{65.125}$$

$$n = \mathbf{394}$$

The 394 sample size represents the minimum number of TEVETA examination candidates that were eligible to participate in the study.

3.2.3 Data Collection

The researcher sought authority from respective TEVETA registered institutions before collecting quantitative data. Furthermore, the researcher sought authority from the IT Manager at TEVETA before collecting quantitative data from Data Entry Personnel and other IT staff. Interviews were also conducted some ICT staff at TEVETA. The data collection exercise lasted for four (4) weeks.

3.2.4 Data Analysis

Quantitative data was analysed through Microsoft Excel application program. The results were presented using charts, graphs and tables.

3.2.5 Ethical Consideration

Respondents were assured of confidentiality from their responses as this research was for academic purposes.

3.2.6 Limitations of Baseline Study

The researcher did not have sufficient money and time to carry out research in all the ten (10) provinces of Zambia.

3.3 System Automation

The results of the baseline study were used to design a model based on current business processes for candidate registration and dissemination of examination results. A prototype based on the model was developed. The proposed model utilizes AES encryption algorithm and SHA3-224 cryptographic hash algorithm during storage and transmission of examination results in order to provide confidentiality, integrity and authenticity of examination results. The proposed model is expected to reduce the time it takes for students and other stakeholders to access TEVETA

examination results. Furthermore, the model provides secure storage and transmission of examination results.

Interviews conducted with IT staff helped to understand how registration for examinations and dissemination of results are done, and then a model was designed for the proposed system. Questionnaires administered to TEVETA Data Entry helped to understand the challenges in candidate registration for examinations and dissemination of examination results.

3.3.1 Current TEVETA Business Processes

The candidate registration process begins by candidates filling in a registration form. The registration forms are filled in by first year students only. The process of registration takes place between January and March. Candidates are required to submit the filled in registration forms to the examination officer or any staff in charge of examinations at their institution of study. The examination officer or staff in charge of examination then enters data in a spreadsheet. The candidate details are printed and then sent to TEVETA along with registration forms. At TEVETA, a desktop application is used to capture candidate details, process and print control sheets. The control sheets are sent to respective institutions of study for verification of the entries. Candidates are required to verify their details and make amendments in case some details are incorrect. The amended control sheet is sent back to TEVETA for corrections. A final register inclusive of examination numbers are then printed and sent to respective institutions of study. Figure 4 is a diagrammatical representation of the current TEVETA business processes for candidate registration.

Candidates are required to fill in examination entry forms before sitting for examinations. Filled in examination forms are then submitted to the examinations officer or staff in charge of examination at candidate's institution of study so that data can be captured into a spreadsheet and later printed. The printed document is sent to TEVETA together with the examination entry forms for data entry and processing. After processing, TEVETA prints registers and dockets for students. The dockets and

registers are sent to respective institutions of study during the examination period. After candidates write examinations, they are marked, results are graded and then released.

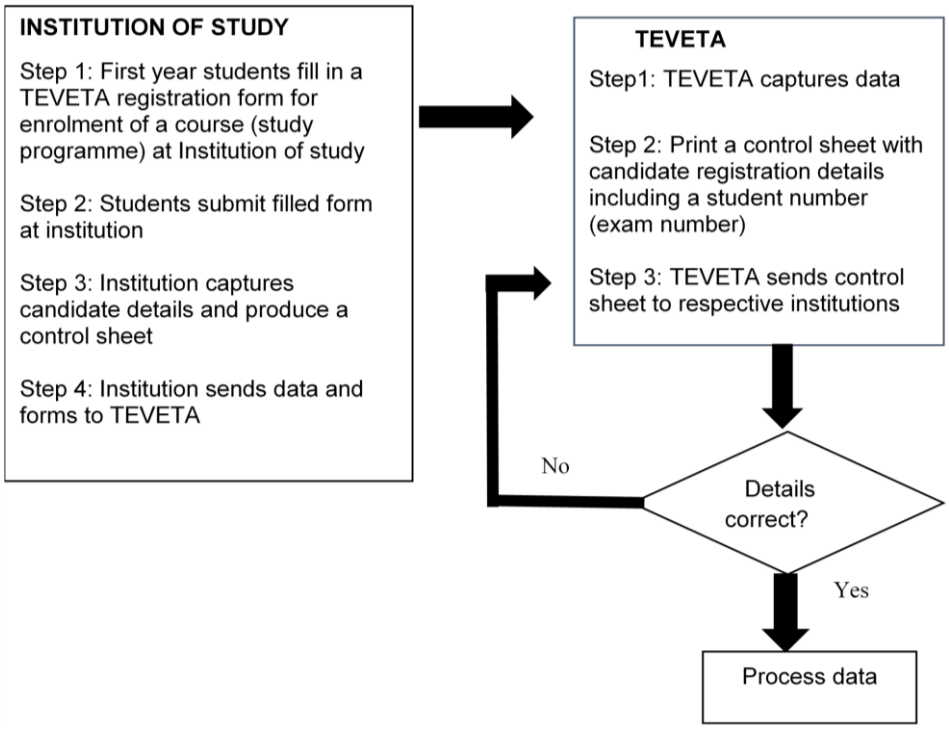


Fig. 4: Current TEVETA business processes for candidate registration

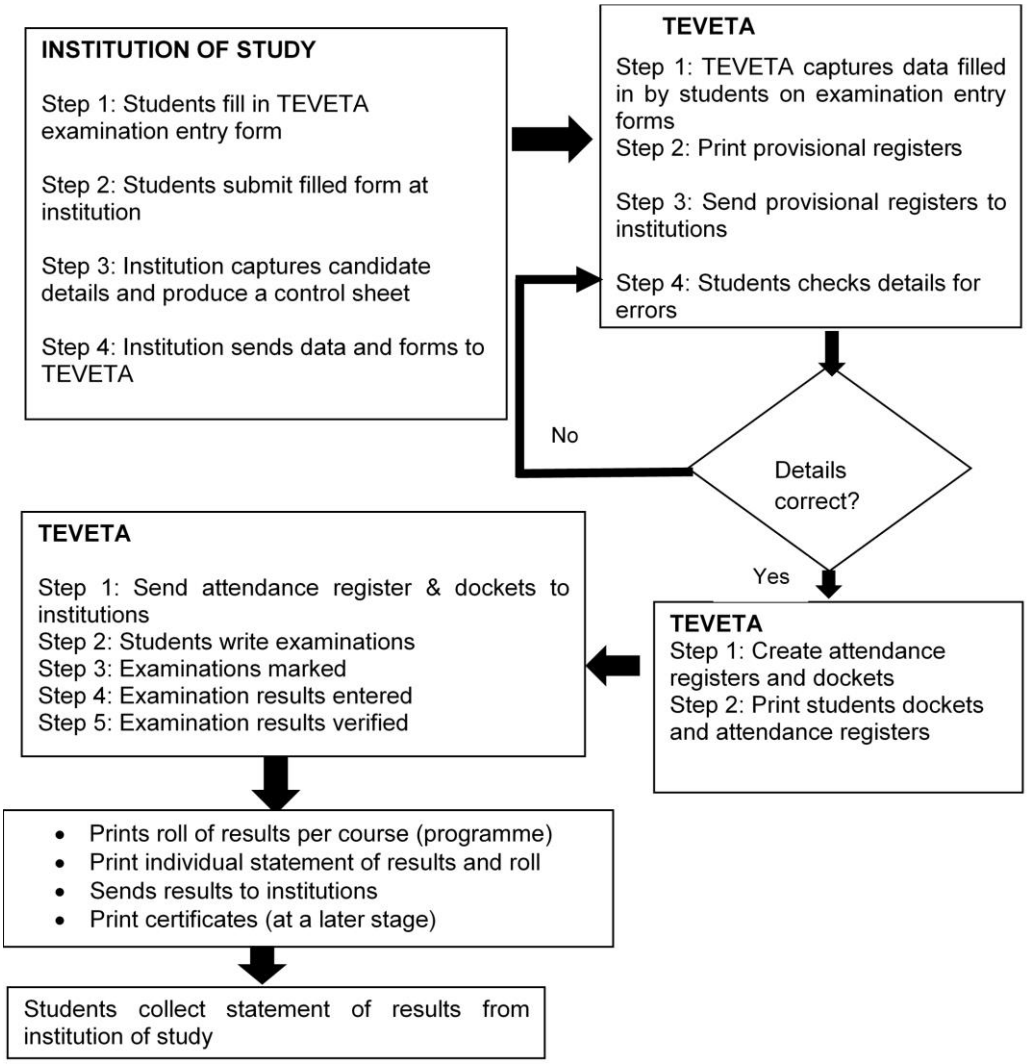


Fig. 5: Examination registration and dissemination of results business processes

3.3.2 Business Process Mapping

The proposed secure model in Fig.6 is derived from the current TEVETA business processes for (candidate registration, examination results entry, verification, publishing and dissemination of results) and ISO 27001 information security standard for access control. A web and mobile prototype for dissemination of students' examination results using AES encryption algorithm and SHA3-224 cryptographic hash function based on the model was then developed. A web and mobile prototype based on the model in Fig.6 provides an avenue for confidentiality of students' examination results through encryption as well of integrity and authenticity of students' examination results through detection of altered students' examination

results during transmission and storage using cryptographic hash function.

Proposed Secure Model for Examination Results Storage and Dissemination

The system architecture consists of four sub sections: the registration phase, entering of marks, verification and publishing of results, and dissemination of examination results as shown in Fig.6. The registration phase involves capturing candidate information by TEVETA. All details pertaining to registration are stored in the database. After a candidate sits for examinations, marks are entered. Each plain text mark is encrypted and hashed with AES encryption algorithm and SHA3-224 algorithm respectively so that the final encoded mark consists of two parts; an encrypted mark and a hashed mark. Hashed marks and encrypted marks are then stored in different databases for the purpose of adding another layer of defence on examination results. During retrieval of student marks, SHA3-224 is used to check the integrity of each stored encrypted mark in the database. The process involves decrypting each mark with AES encryption algorithm, hashing each mark with SHA3-224 and then comparing the hashed mark with the hashed mark originally stored in database. If the two hashes of marks match, the application proceed to display the examination results, otherwise it will return an alert as it is an indication that marks were altered while in transit or storage and therefore are not authentic.

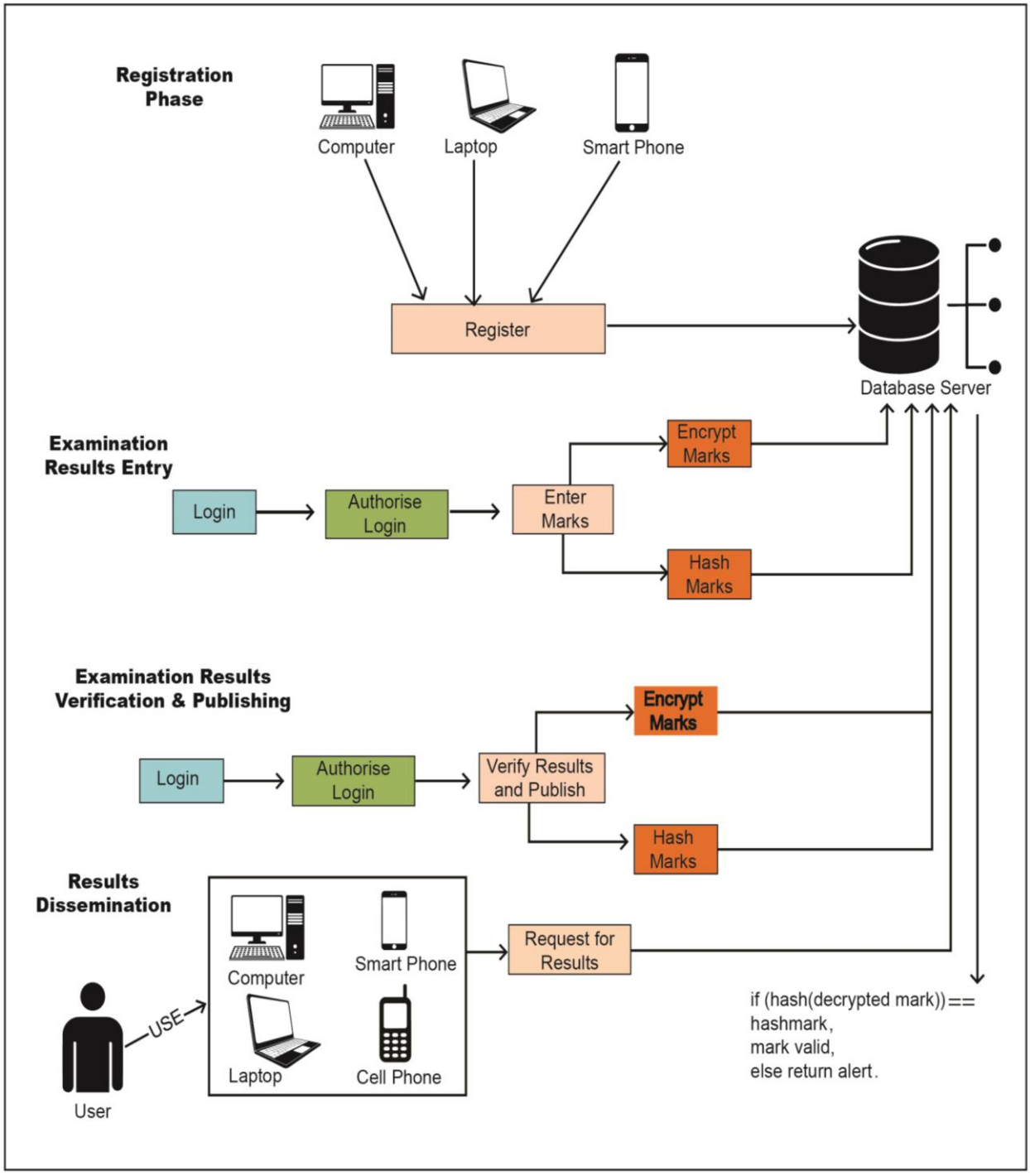


Fig. 6: Secure architecture for examination results storage and dissemination

3.3.3 Secure Models for Examination Results Entry and Retrieval Definition

Cryptographic hash functions provides the assurance of data integrity with the notion of an imprint of a fingerprint on source data, that any alteration in transit or on the

database (storage) no longer guarantee the integrity of data. Let h be the hash function and m the mark, then the corresponding fingerprint or message digest is defined as:

$$x = h(m) \qquad \text{Equation } \textbf{\textit{(5)}}$$

if x is stored in a secure place, then

$$y = x \qquad \text{Equation } \textbf{\textit{(6)}}$$

If the source data, m is changed in transit or on the database, it becomes m', then the corresponding message digest in equation ***(5)*** will change from x to x' as:

$$y = x \qquad \text{Equation (7)}$$

If marks are altered in transit or on the database, then by comparing equation ***(6)*** and *(7)* it can be deduced that:

$$y \neq y' \qquad \text{Equation (8)}$$

verifying that the integrity of the marks have been compromised.

The algorithm for secure insertion of examination results using AES encryption and SHA3-224 works as follows:

start:
mark1 = aes_encrypt (mark, key)
mark2 = sha3-224(mark)
populate table in database (A) and table in database (B) with mark1 and mark2 respectively
stop.

During retrieval of results, the SHA3-224 works as follows:

Start:
Retrieve mark 1 and mark 2 from database (A) and database (B) respectively
Mark1 -----> (encrypted mark)
Mark2 ------> (hashed mark)
Mark3 = AES_DECRYPT (mark1, key)
hashedmark = SHA3-224(mark3)
Compare mark2 with hashedmark,
If hashedmark equals mark2
Display results
Else return alert
Stop.

Figure 7 shows secure examination entry while Fig. 8 shows the diagrammatic flow of results integrity check during retrieval of examination results.

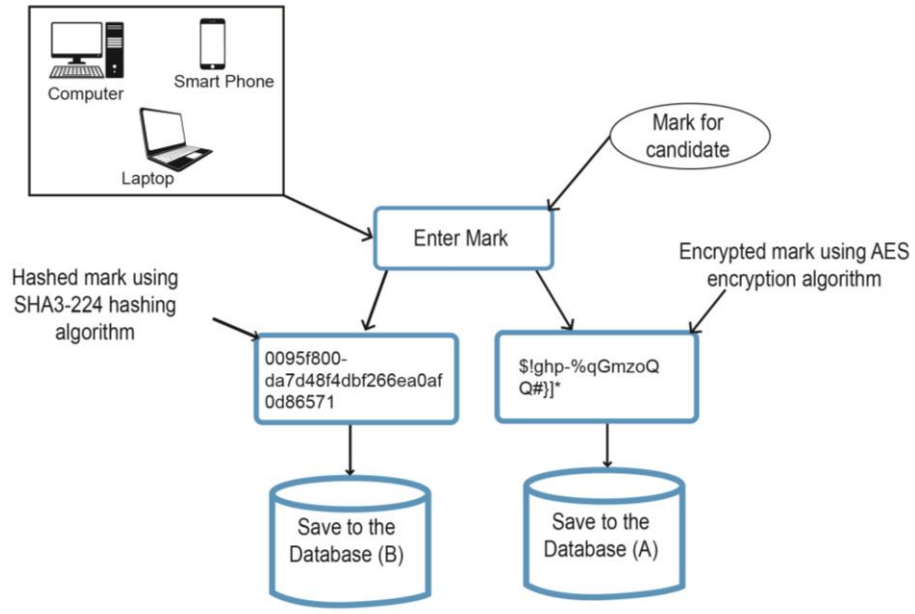


Fig. 7: Secure architecture for insertion of student results

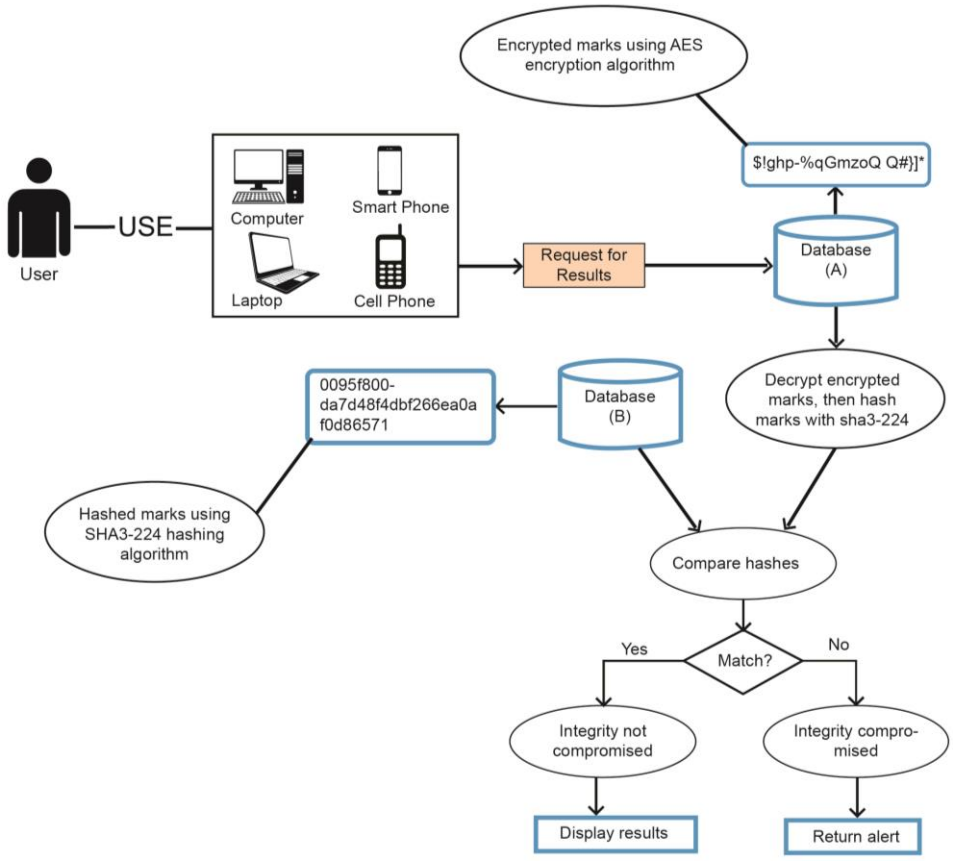


Fig. 8: Secure architecture for retrieval of examination results

3.3.4 System Requirements Specification

Requirements specification is an important aspect of system development as it specifies in a complete and concise manner, the expected behaviour or characteristics of the software to be developed. There are two categories of requirements: functional and non-functional requirements. Functional requirements are concerned with functions and services to be performed by the software while non-functional requirements are concerned with the constraints under which the software must operate, such as user friendliness, response time, and memory usage [98].

Functional Requirements

Table 3 describes functional requirements for the system.

Table 3 Functional requirements

FR1	*Users with the relevant access rights can register a candidate for examinations in a particular year at a specific institution of study.* Such users are data entry personnel or any other person assigned with this role at TEVETA.
FR2	*Users with relevant access rights can update candidate records both personal details and update subject entries.*
FR3	*Users with relevant access rights can delete candidate records both personal details and update subject entries.*
FR4	*Users with relevant access rights can delete candidate records both personal details and update subject entries* shall be able to generate reports such as provisional registers, statistics such as number of students who failed or passed, statement of results for candidates in respective institutions of study.
FR5	User shall be able to view candidate registration data. Such users shall include data managers or any other person assigned this role at TEVETA. Students with relevant access right can view their registration details.
FR6	*Users with relevant access rights can enter examination results for candidates.* Such users are data entry personnel or any other person assigned with this role at TEVETA.
FR7	*Users with relevant access rights can update examination results for*

	candidates. Such users include data managers or any other person assigned with this role at TEVETA.
FR8	*Users with relevant access rights can verify and publish examination results for candidates.* Such users include data managers or any other person assigned with this role at TEVETA.
FR9	*The system shall check against the database whether the hash of the decrypted mark extracted from the database match with the hash stored in the database during retrieval of examination results.* If the hashes match, the system shall proceed and allow results to be decrypted and displayed. If the hashes do not match, the system shall give an alert, indicating that examination results have been illegally modified.
FR9	*User with relevant permission can view examination results for a candidate*. This includes students (owner of examination results), employers, universities or any other interested stakeholders.
FR10	*Users with relevant access rights can change their passwords at any time.*
FR11	*The system administrator shall be able to create new system users.*
FR12	*The system administrator shall be update a user's access permissions*.
FR13	*The system administrator shall be able to delete a user from the system.*

Non-functional Requirements

Table 4 details non-functional requirements for the system.

Table 4 Non-functional requirements

NFR1	*System failure shall not compromise examination results or candidate registration data integrity.*
NFR2	Encryption shall be ensured at all interfaces where data could be intercepted or transmitted.
NFR3	*The system shall be user friendly.* Drop down menus, meaningful error messages, prompts shall be provided.
NFR4	*All software application modules shall be debuggable.*
NFR5	*All input and output, storage and retrieval operations shall efficiently use system resources to reduce overload.*
NFR6	*All users using the system shall log in with some form of unique identification*

	(e.g. unique exam number, employee number or username and password).
NFR7	*All login attempts shall be done in a secure manner* (e.g. passwords shall be hashed)
NFR8	*Software shall be written in a style that is easy to read through use of comments and code shall be well documented*
NFR9	*Documentation of all functionality and software maintenance shall be provided.*
NFR10	*All future upgrades to the system shall be accompanied with full explanatory documentation.*
NFR11	*Operating system, message passing and programming language (s) used shall follow industry standards and be commonly available and widely used.*
NFR12	*A systems administrator shall have unrestricted access to the system except creation of candidate records, entering marks, updating and publishing of examination results.*
NFR13	*Each group of users have specific access properties that defines user's privileges within the system.* For example, a candidate cannot view another candidate's registration details or examination results.

3.3.5 System Modelling

Object Oriented Design (OOD) was used to analyse the existing system and design the system modules. Unified Modelling Language was used in this study as it is the de facto standard for object oriented systems [98]. UML diagrams are categorized in two, namely: behavioral and structural diagrams. Behavioral diagrams depict the dynamic behavioral while structural diagrams depict the static behavior of the software system. In this study, class diagrams and were used to capture the static behavior of the software system while use cases and activity diagrams were used to capture the dynamic behaviors of the software system.

Use Cases

Use case diagrams describe the functionality of the system from the user's perspective. The main actors in candidate registration and examination results

processing are the system administrator and the user (Data Entry Personnel, Data Manager and other authorised personnel). Table 5 shows the actor - User, use cases and description.

Table 5 Use cases and descriptions

Use Case	Actor	Description
Login	User	A registered user can log in to access system functionality according to his or her access rights using his or her credentials
Register candidate	User	Users with relevant access rights can enter candidate details such as candidate examination number, name, date of birth, national registration card number, institution of study, programme of study, nationality, and passport where applicable
Update Candidate Details	User	Users with the appropriate rights can update candidate details of a registered candidate such as candidate name, sex, date of birth, programme of study, institution of study, nationality, and passport where applicable
Enter Results	User	Users with appropriate permissions can enter examination results for candidates
Verify/Edit Results	User	Users with appropriate permissions can verify examination results for candidates. If mark entries are incorrect for a candidate, the user can edit the results.
Authorise Results	User	Users with appropriate permissions can authorise examination results for candidates so that other users with relevant permissions can perform a number of operations on them e.g. publish results or generate transcripts
Publish Results	User	Users with appropriate permissions can publish examination results for candidates so that students and other stakeholders can view results
Generate Transcript	User	Users with appropriate permissions can generate transcripts for candidates
Generate Report	User	Users with relevant access rights can generate and print various reports about registered candidates
Verify Transcript	User	Users with appropriate permissions can verify transcripts for candidates
View Registration Data	User	All logged in users are able to view candidate registration details through a user interface based

		on their access rights. For example, a student can only view their own enrolment details, while managers for respective programmes can view candidate details for their specialist and the data manager can view all candidate details regardless of the specialization.
View Results	User	Users with appropriate permissions can view examination results for candidates based on their access rights. For example, a student can only view their own examination results, while the data manager can view all examination results for candidates.
Logout	User	Logs out to close the opened session

Figure 9 is a diagrammatical representation of the actor – User and the use cases associated to this actor.

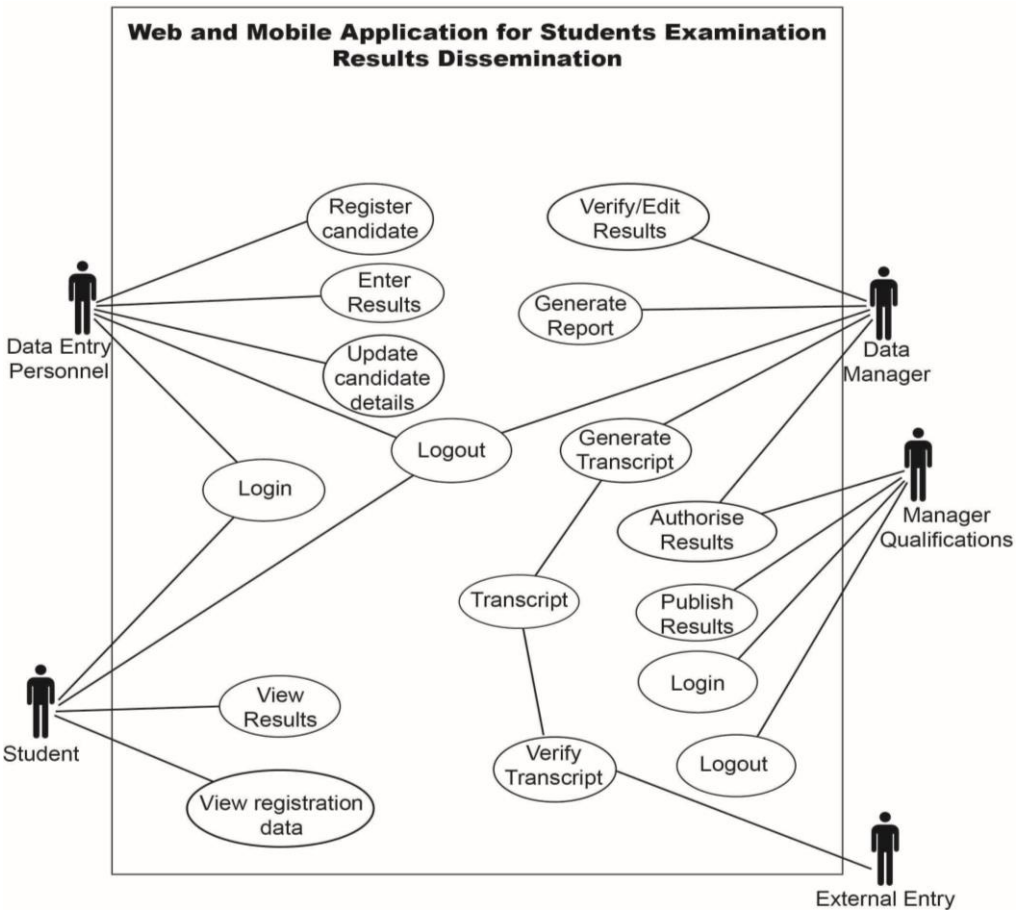


Fig. 9: System Use Case Diagram

Table 6 shows the actor (system administrator), use cases and description.

Table 6 System administrator use cases and descriptions

Use Case	Actor	Description
Login	Administrator	Validates credentials and opens the page for the systems administrator
Create User Account	Administrator	When a new member of staff joins the unit for candidate registration, examination results entry and management, his or her details are added to the database,
Manage User	Administrator	Manage user accounts
Update User Account	Administrator	Edits user accounts when there are changes
Delete User Account	Administrator	When a user leaves the unit for candidate registration, examination results entry and management, the administrator deletes him from the database
Change Password	Administrator	Change the password
View User	Administrator	View account details for users
Log out	Administrator	Logs out to close the opened session

Figure 10 is a diagrammatical of how system administrators interact with the system.

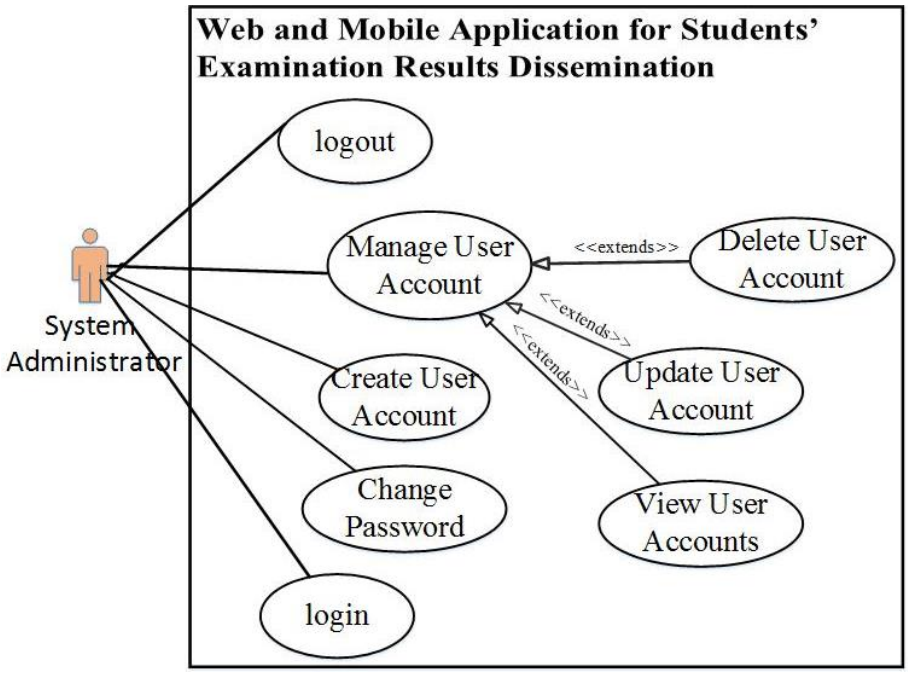


Fig.10: System Administrators use case diagram.

Class Diagram

Class diagrams describe the static structure of the system showing the relationship between objects. Figure 11 is a class diagram depicting static relationships that represent the fundamental architecture of the system.

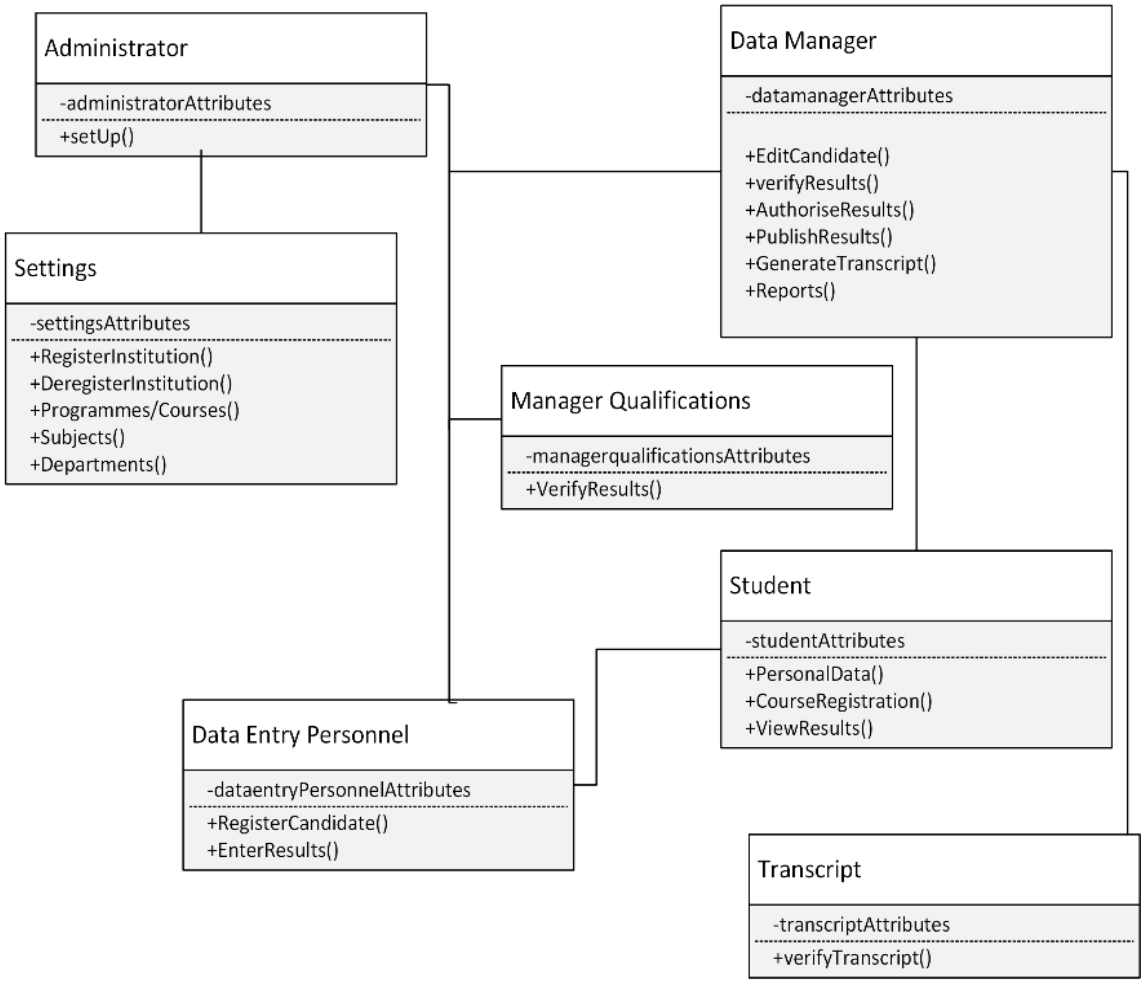


Fig. 11: Class Diagram for Examination Results

Activity Diagram

Activity diagrams are used for modelling the logic captured by a single use case, or for modelling the detailed logic of a business rule. The activity diagram in Fig.12 shows the result computation process. The process of computing student results is performed by three roles which begins with the Data Entry personnel who enters the score of the students. The results are queued waiting for authorisation by the Data Manager which is the first level of authorisation. The Manager Qualifications performs the second level of authorisation. In the event that authorisation is denied at

any level, results are removed for and sent to relevant personnel for reconsideration. Otherwise, the Data Manager can generate results for consideration by Senate or committee responsible for results. Upon approval by Senate or committee, manager qualifications or any personnel charged with the responsibility can publish results for students and other stake holders to view.

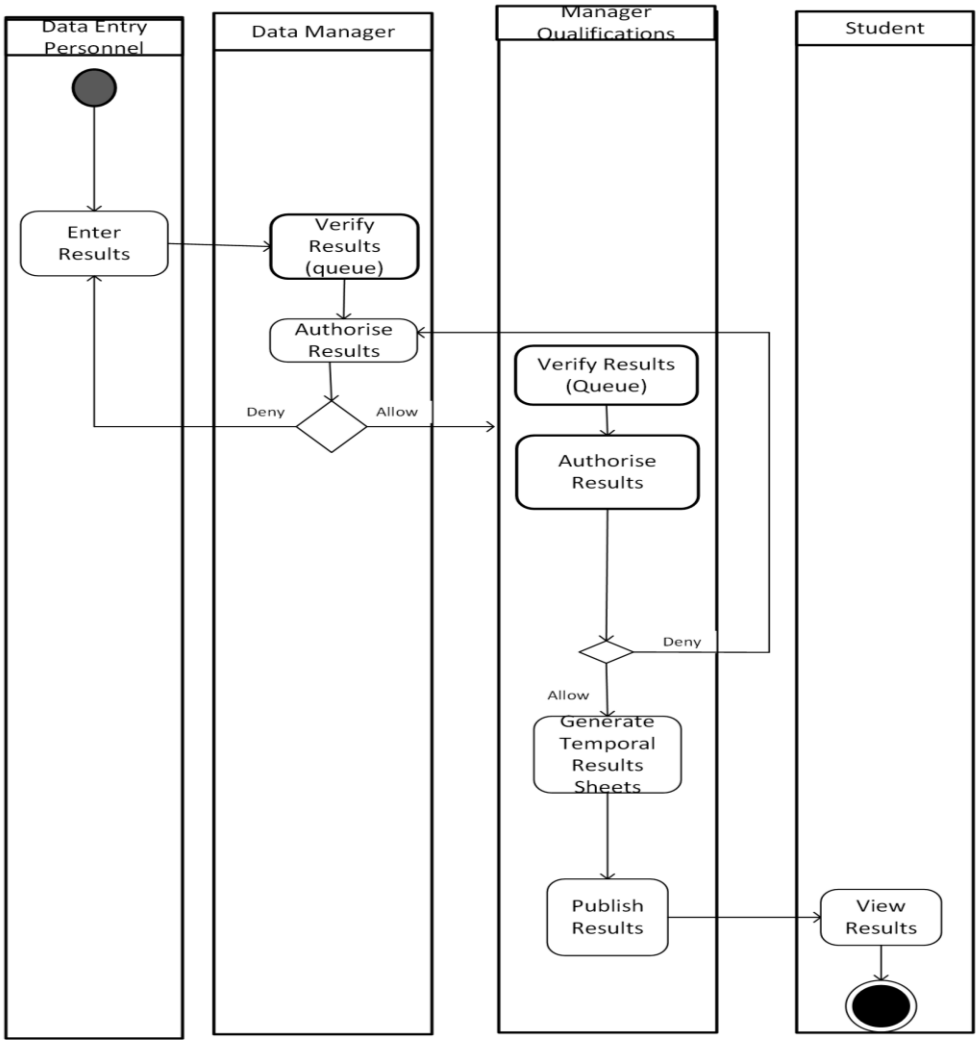
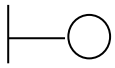


Fig. 12: Activity diagram for Results Computation process

Interactive models – collaboration (communication) and sequence diagrams

Communication diagrams show the interaction between objects while sequence diagrams on the other hand, depict object interactions by highlighting the time ordering of method invocations [98]. This section details the communication and sequence diagrams for each use case depicted in Fig.9.

Table 7 Sequence and collaboration diagram symbols [98]

Symbol	Description
	Boundary object: Objects that interface between a system and its actors
	Control object: objects that mediate between boundaries and entities.
	Entity objects: Objects representing system data, from a real life objects

Login

In Fig.13, the login user interface is started. The control object prompts the user to enter their credentials and authenticates the user upon furnishing the correct login credentials. It then asks the User entity object to get the user account from the user account from the database. The control object finally asks the boundary object to display the welcome screen to the user at the application interface.

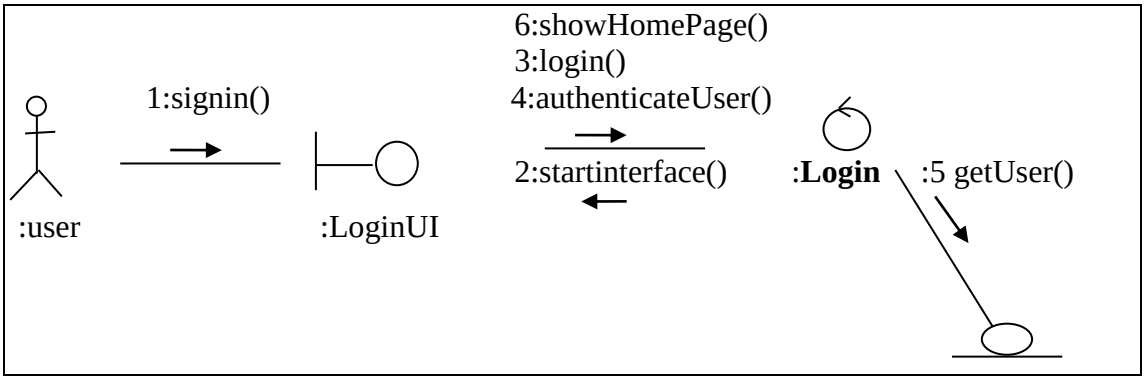


Fig. 13: Login communication diagram

The sequence diagram in Fig.14 is a synchronization of the communication diagram in Fig.13. The sequence of events for the LogIn use case are shown in Fig.14.

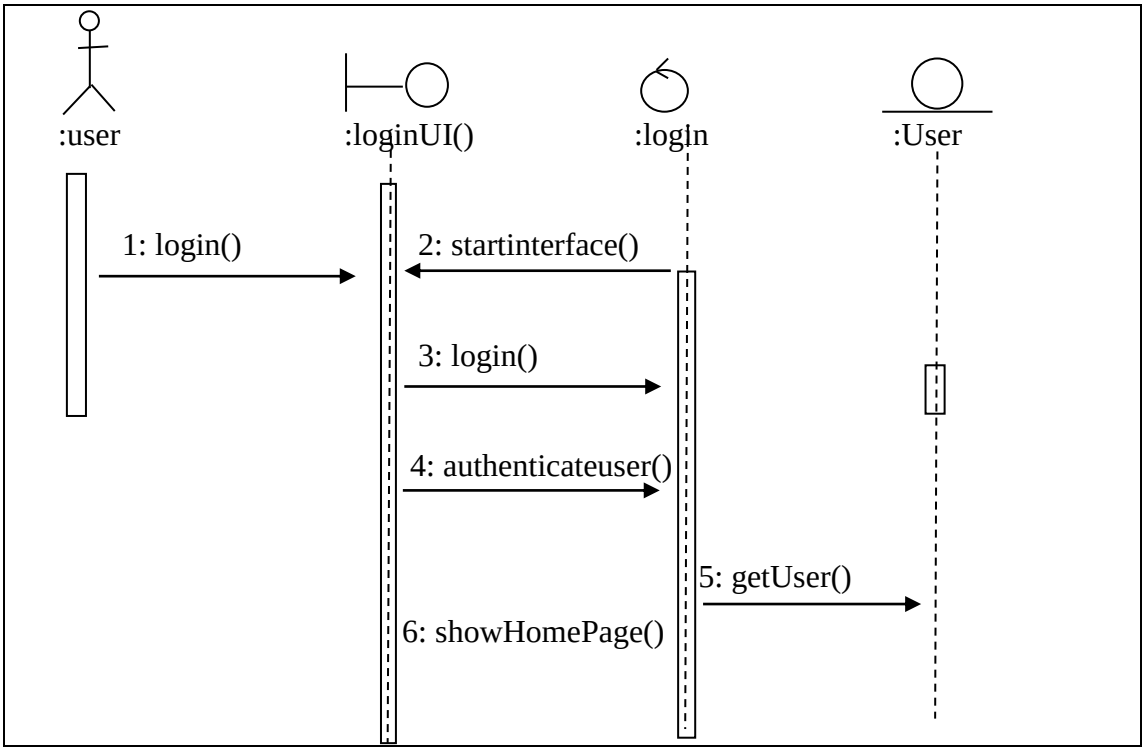


Fig. 14: Login sequence diagram

In Fig. 15, the User Interface (IU) is started and then the control object is instantiated. The selects the menu to register a candidate and the system automatically generates an examination number for the user to enter candidate personal details. If the candidate is registering for examinations in advanced levels, then the user enters an examination number and then the control object validates the examination number and retrieves candidate's details. The user then enters the level and the candidate is automatically enrolled to sit for examinations in a level selected. The control object finally asks the boundary object to display that a candidate has been successfully registered.

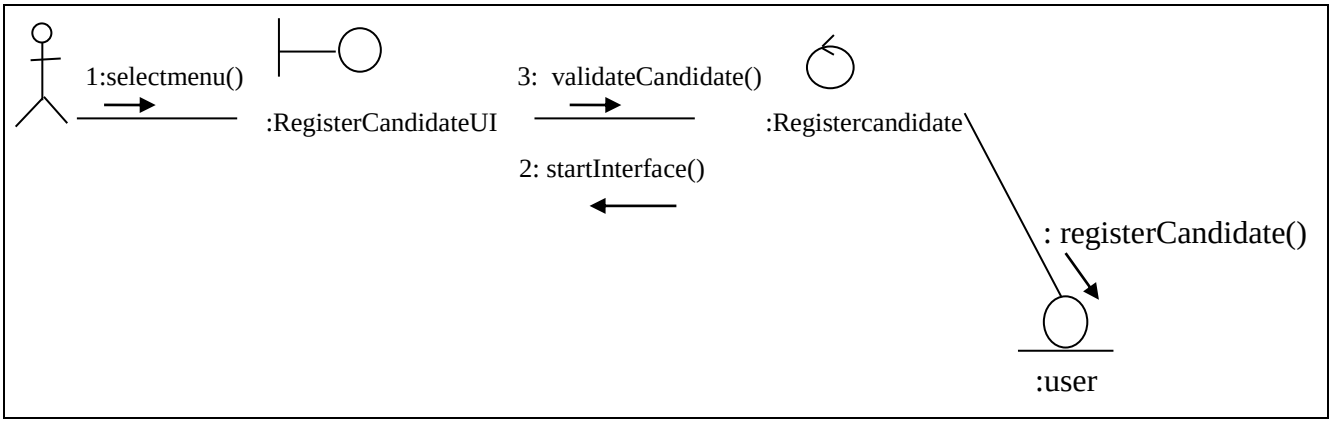


Fig. 15: Register Candidate communication diagram

The sequence diagram in Fig.16 is a synchronization of the communication diagram in Fig.15. The sequence of events for the Register Candidate use case is shown in Fig. 16.

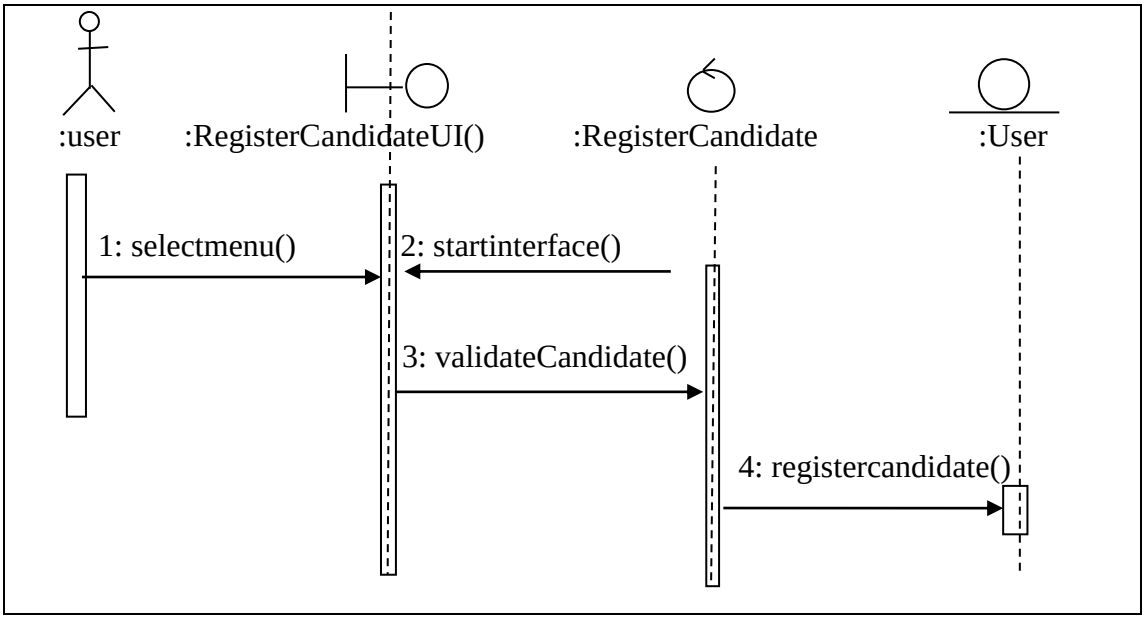


Fig. 16: Register Candidate sequence diagram

Update Candidate Details

In Fig.17, the User Interface is started and then the control object is instantiated. The User enters the examination number for the candidate they want to edit, the control object gets candidate records from the candidate entity object. The User modifies the details and then the control object executes the update candidate transaction.

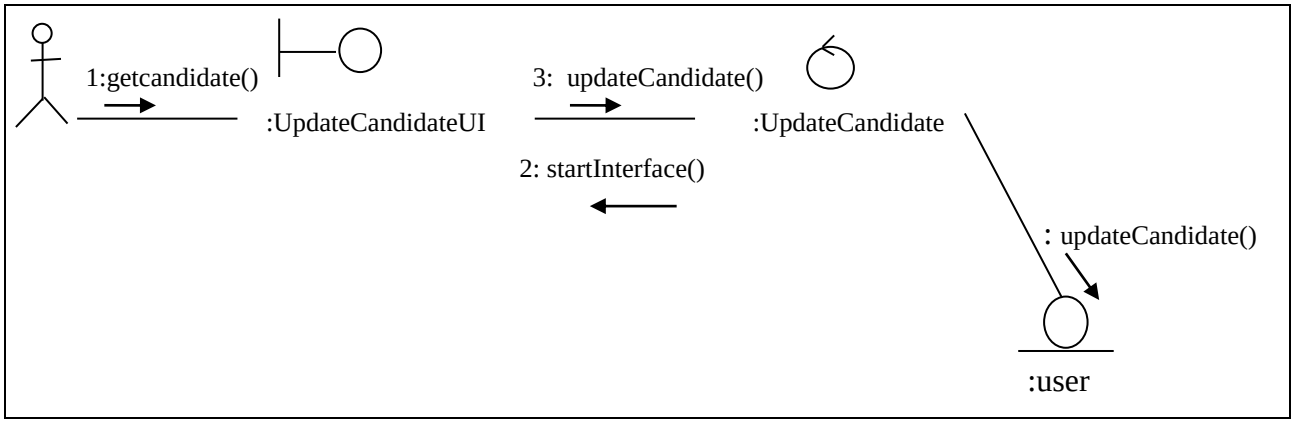


Fig. 17: Update Candidate communication diagram

The sequence diagram in Fig.18 is a synchronization of the communication diagram in Fig.17. The sequence of events for Update Candidate Details use case is shown in Fig.18.

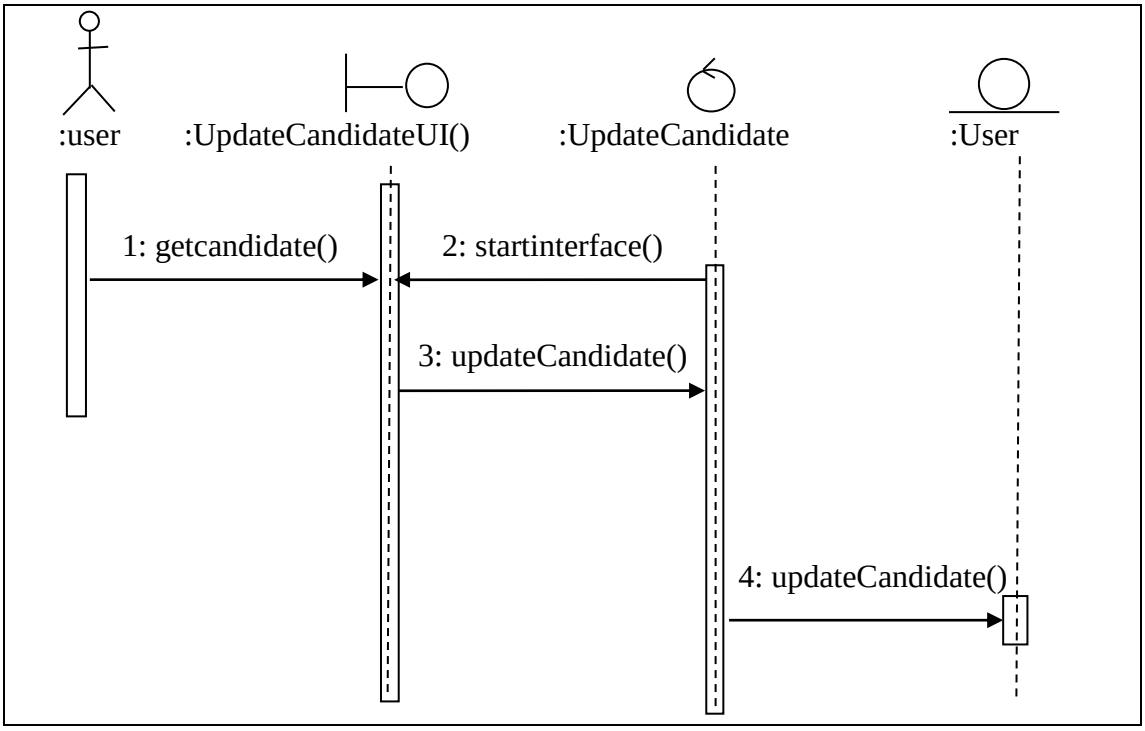


Fig. 18: Update candidate sequence diagram

Enter Examination Results

In Fig.19, the User Interface is started and then the control object is instantiated. The User enters the examination number and level (year) for the candidate they want to enter examination results, the control object gets candidate subject details from the Results entity object. The User enters the results and then the control object executes the transaction.

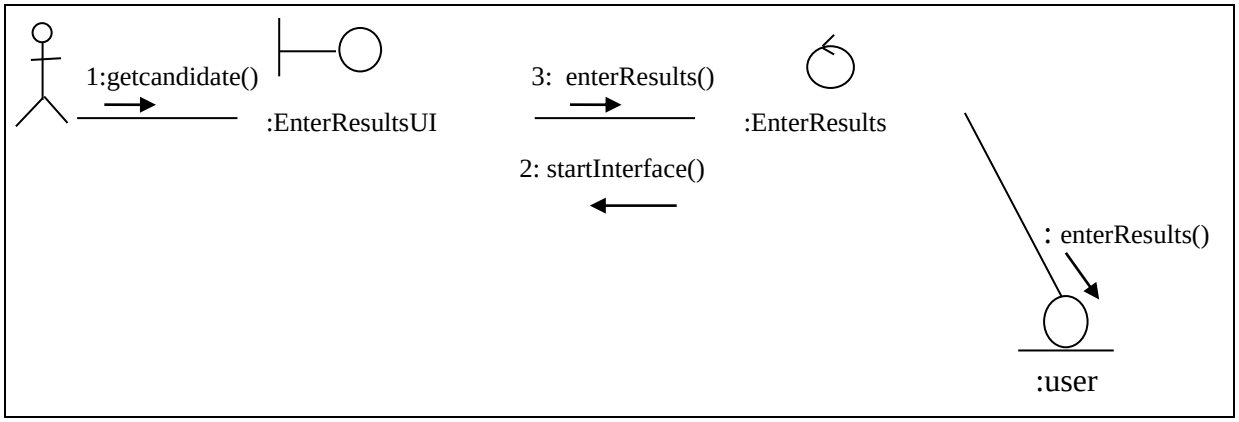


Fig. 19: Enter Results communication diagram

The sequence diagram in Fig.20 is a synchronization of the communication diagram in Fig.19. The sequence of events for Enter Results use case is shown in Fig.20.

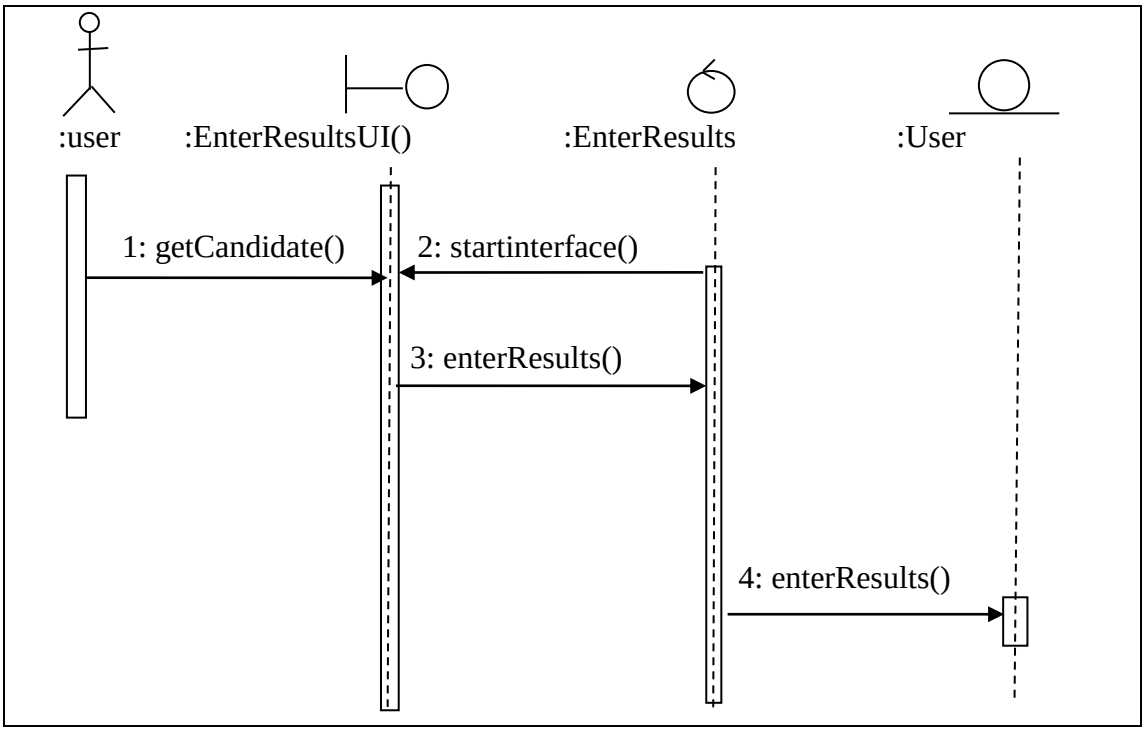


Fig. 20: Enter Results sequence diagram

Verify Examination Results

In Fig.21, the User Interface is started and then the control object is instantiated. The User enters the examination number and level (year) for the candidate they want to verify examination results, the control object gets candidate results from the Results entity object. The User verifies if the results entered are correct, if not, the user edits incorrect mark entries and then the control object executes the verify transaction.

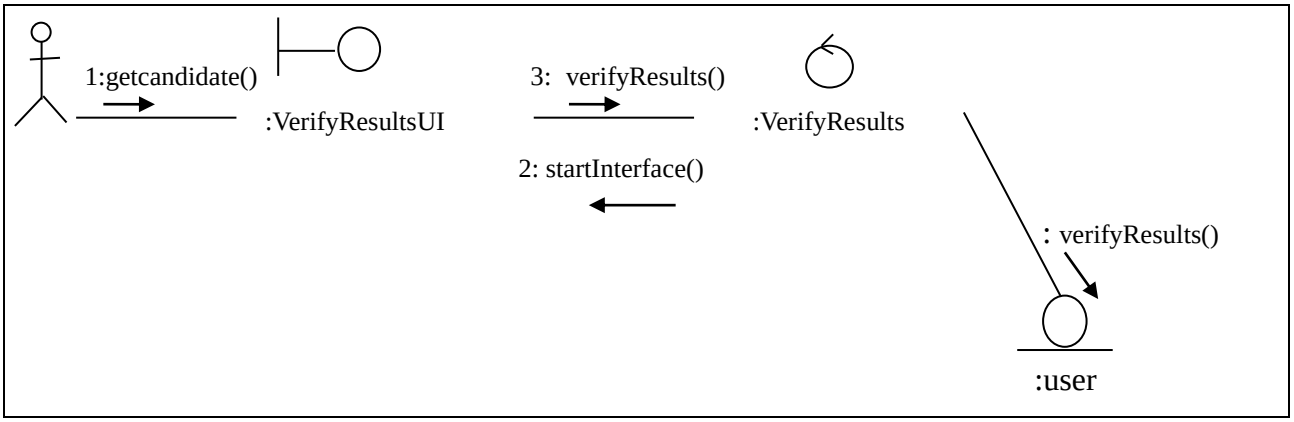


Fig. 21: Verify Results communication diagram

The sequence diagram in Fig.22 is a synchronization of the communication diagram in Fig.21. The sequence of events for Verify Results use case is shown in Fig.22.

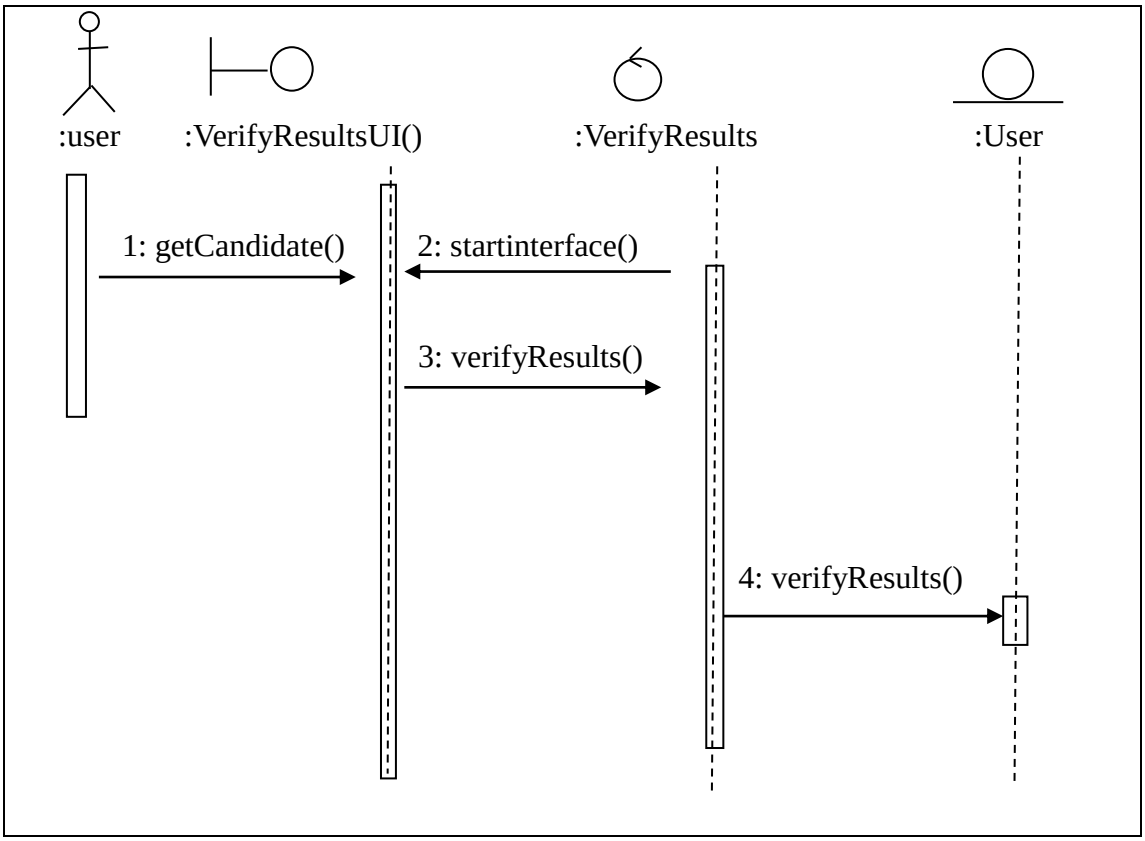


Fig. 22: Verify results sequence diagram

Authorise Examination Results

In Fig.23, the User Interface is started and then the control object is instantiated. The process of result computation is performed by three different roles which begins with the Data Entry Personnel entering/uploading the result score of the students. The result is queued in waiting for the Data Manager's authorisation which is the first level of authorisation. If results are denied authorisation at any level, the result is moved to preceding roles for reevaluation. The data manager can generate results sheets in institution of study form for board of examination results meeting consideration. On approval by the board, the Manager Qualifications can publish the results for students to view.

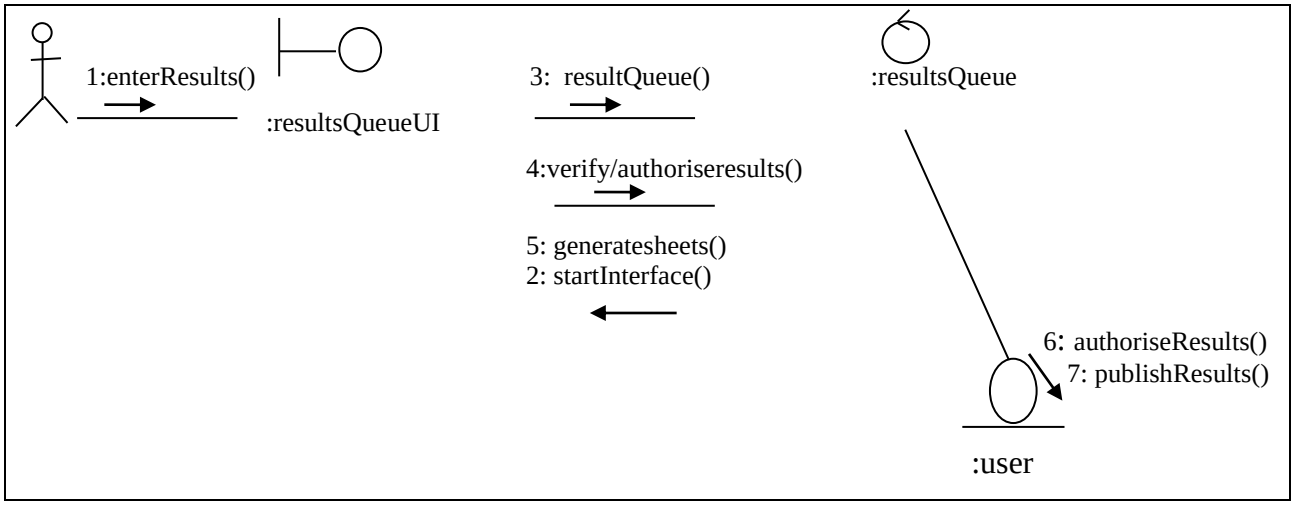


Fig. 23: Authorise Results communication diagram

The sequence diagram in Fig.24 is a synchronization of the communication diagram in Fig.23. The sequence of events for Authorise Results use case is shown in Fig.24.

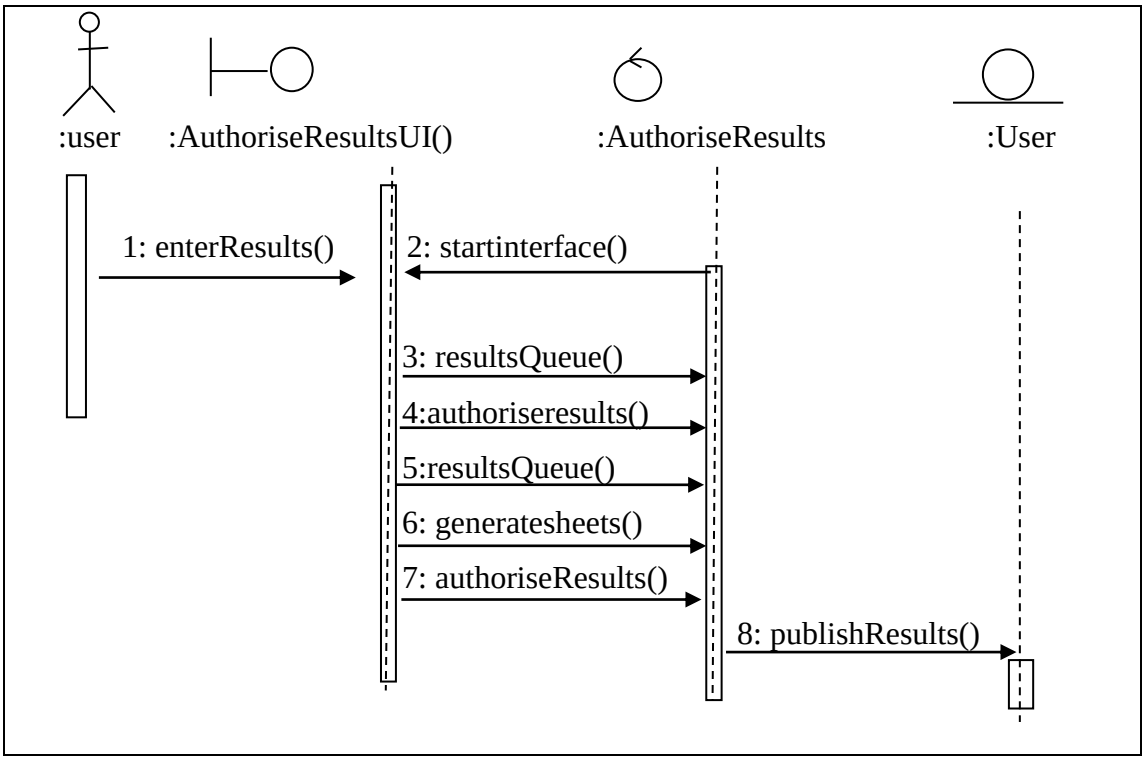


Fig. 24: Authorise Results sequence diagram

Publish examination results

In Fig.25, the User Interface is started and then the control object is instantiated. The User enters the examination number and level (year) for the candidate they want to publish examination results, the control object gets candidate results from the results

entity object. The User publishes examination results and then the control object executes the publish transaction.

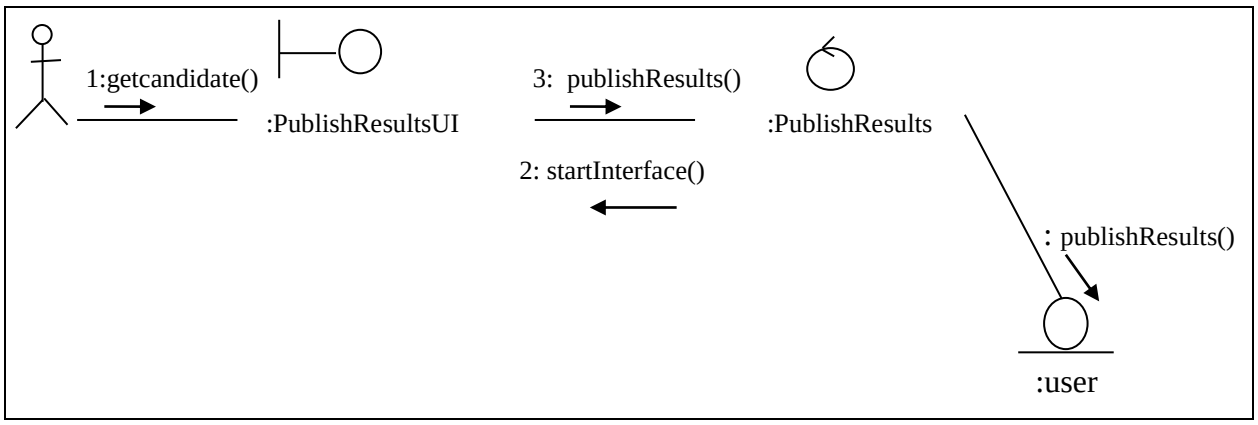


Fig. 25: Publish results communication diagram

The sequence diagram in Fig.26 is a synchronization of the communication diagram in Fig.25. The sequence of events for Publish Results use case is shown in Fig.26.

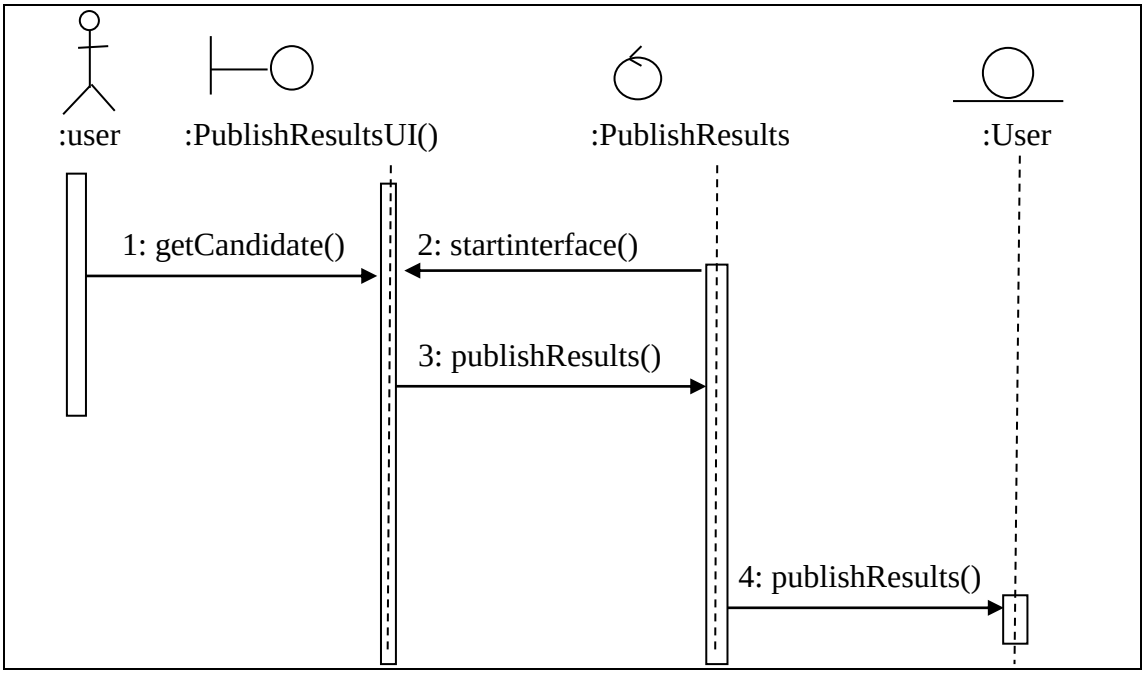


Fig. 26: Sequence diagram for publish examination results

View examination results

In Fig.27, the User Interface is started and then the control object is instantiated. The User enters the examination number and level (year) for the candidate they want to view examination results, the control object gets candidate results from the Results entity object.

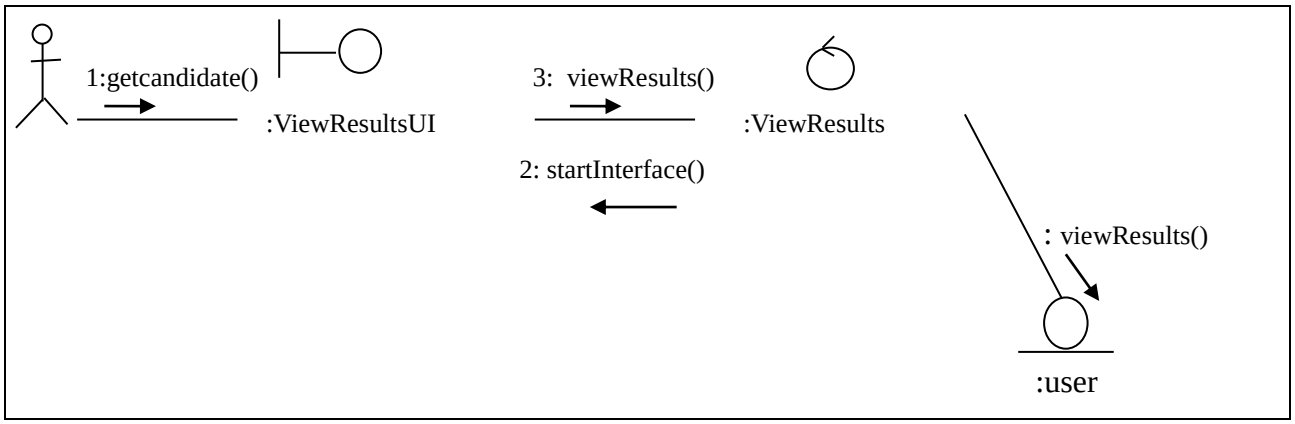


Fig. 27: View results communication diagram

The sequence diagram in Fig.28 is a synchronization of the communication diagram in Fig.27. The sequence of events for View Results use case is shown in Fig.28.

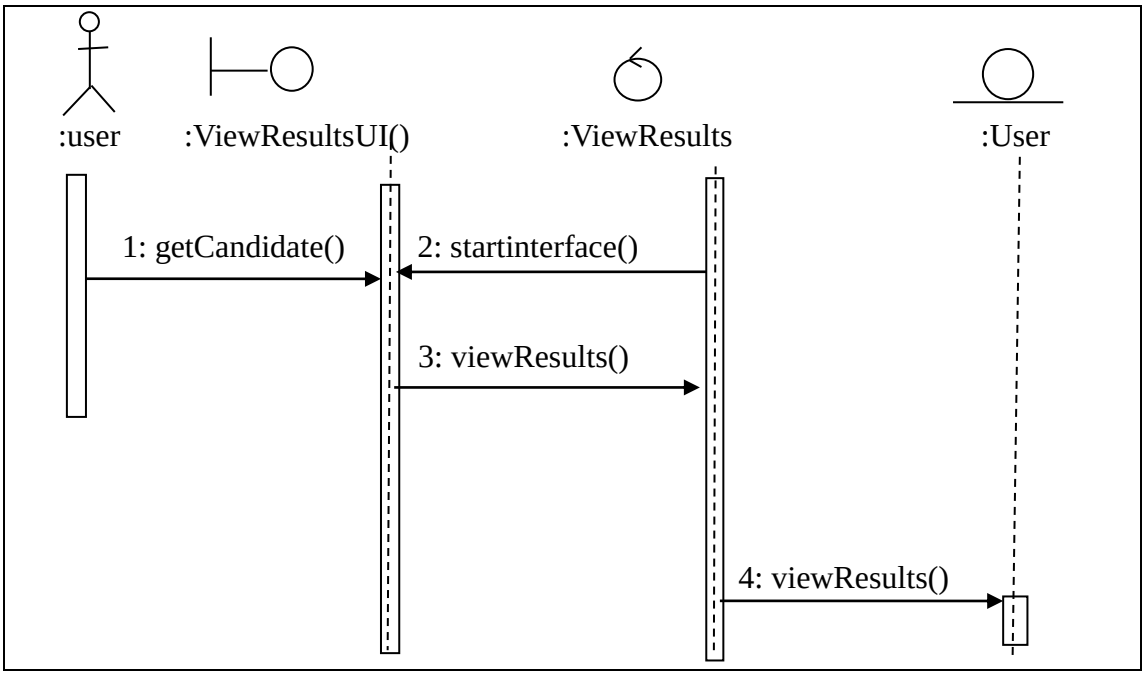


Fig. 28: View results sequence diagram

View Course Registration Data

In Fig.29, the User Interface is started and then the control object is instantiated. The User enters the examination number and level (year) for the candidate they want to view course registration data, the control object gets candidate course (subject) entries from the Results entity object.

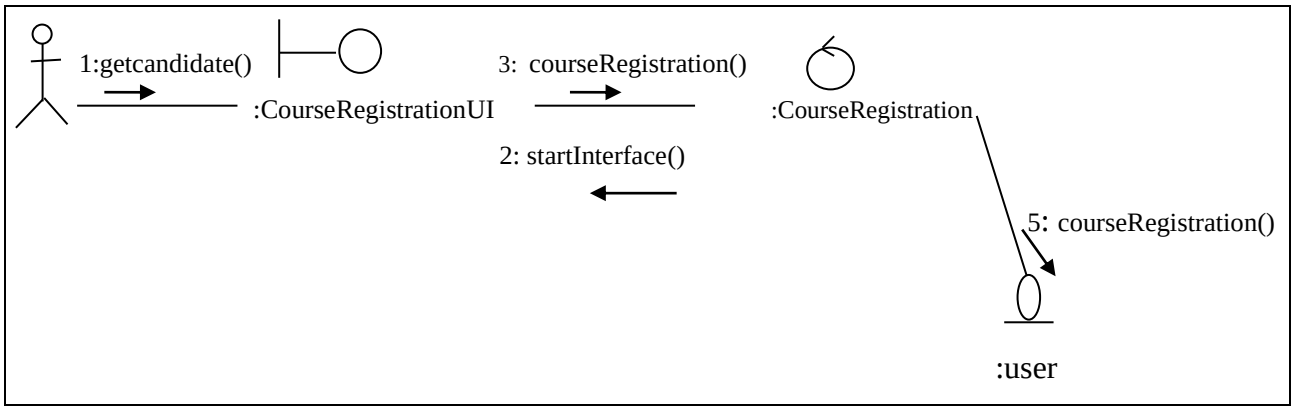


Fig. 29: Course registration communication diagram

The sequence diagram in Fig.30 is a synchronization of the communication diagram in Fig.29. The sequence of events for View Results use case is shown in Fig.30.

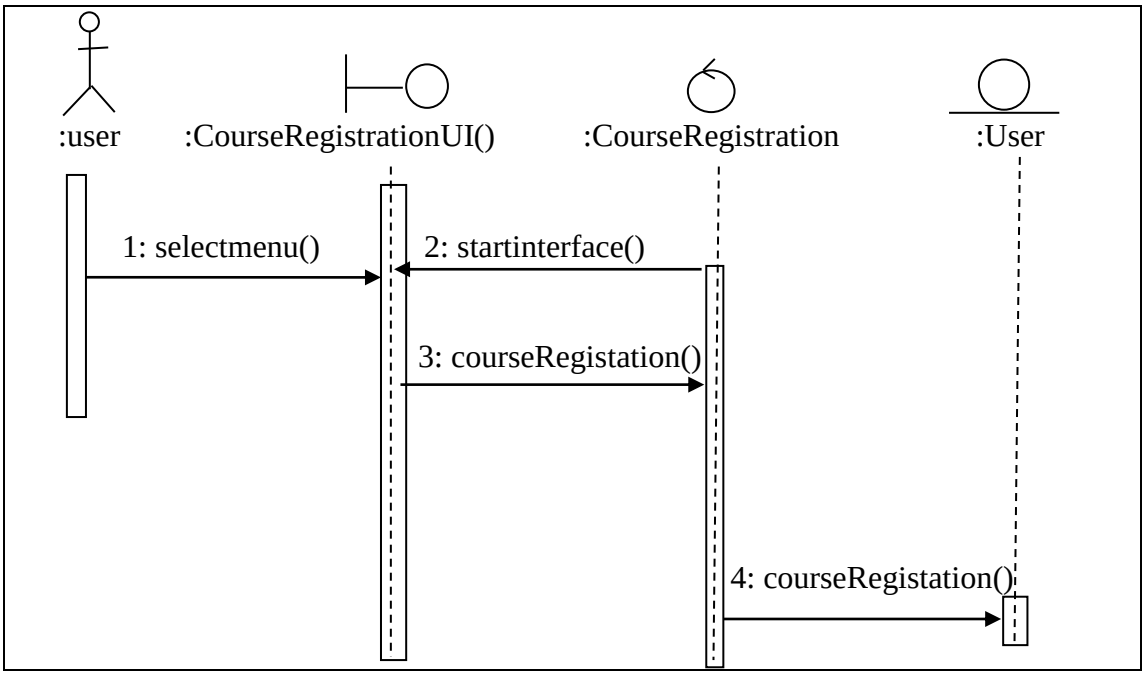


Fig.30: Course Registration sequence diagram

Verify Transcript

In Fig.31, the User Interface is started and then the control object is instantiated. The User enters the examination number and level (year) for the candidate they want to verify the transcript, the control object gets candidate results from the Results entity object.

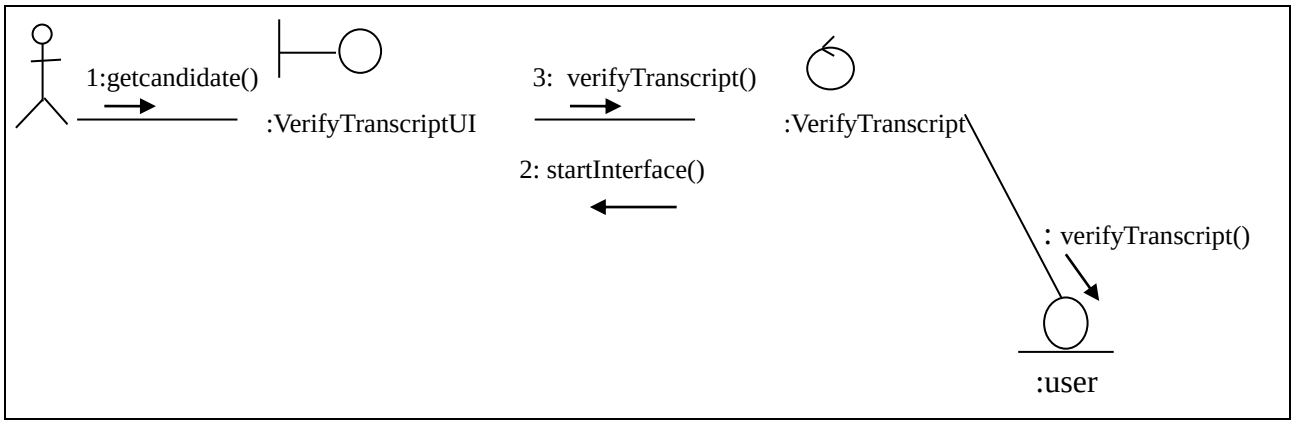


Fig. 31: Verify transcript communication diagram

The sequence diagram in Fig.32 is a synchronization of the communication diagram in Fig.31. The sequence of events for the Verify Transcript use case is shown in Fig.32.

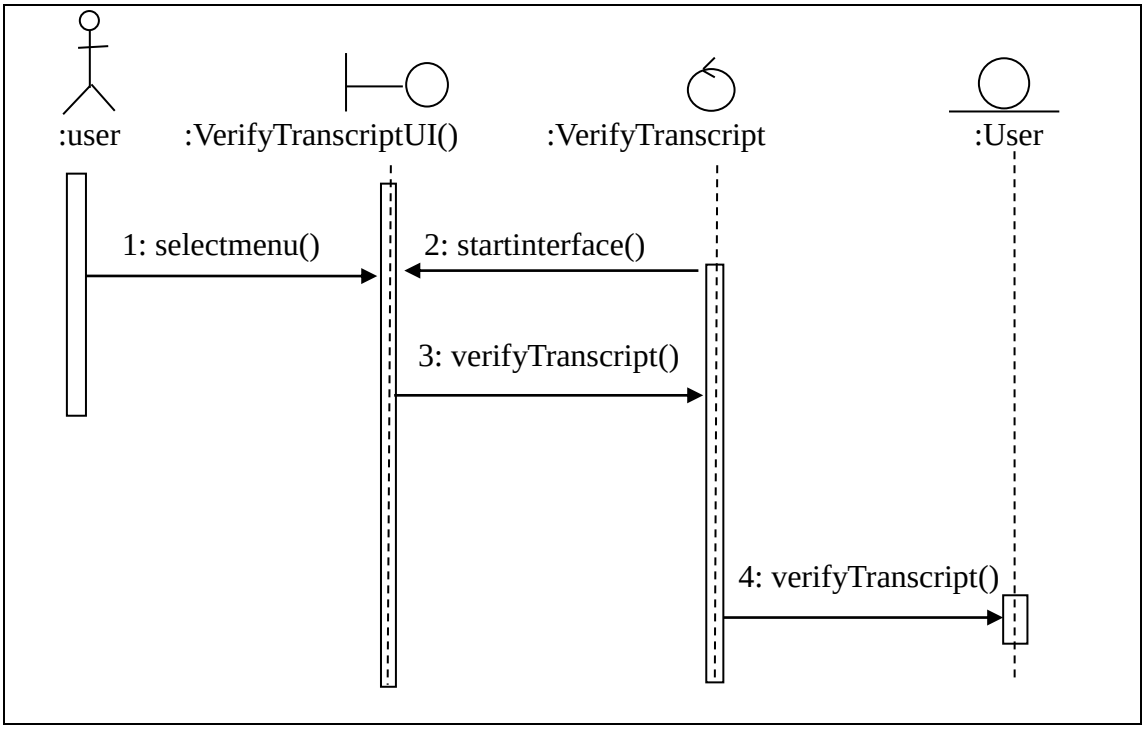


Fig. 32: Verify transcript sequence diagram

Generate Report

In Fig.33, the user selects the type of report they want to generate. The user Interface is started and then the control object is instantiated. The control object executes the generate report and then asks to create the report requested for. The control object

finally asks the boundary object to display the generated report.

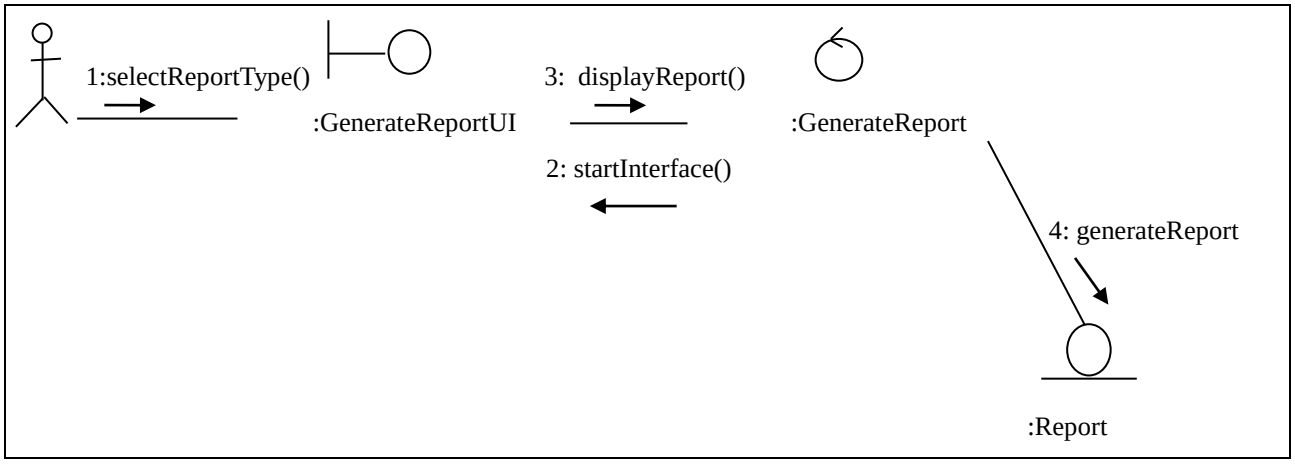


Fig. 33: Generate Report communication diagram

The sequence diagram in Fig.34 is a synchronization of the communication diagram in Fig.33. The sequence of events for the Generate Report use case is shown in Fig.34.

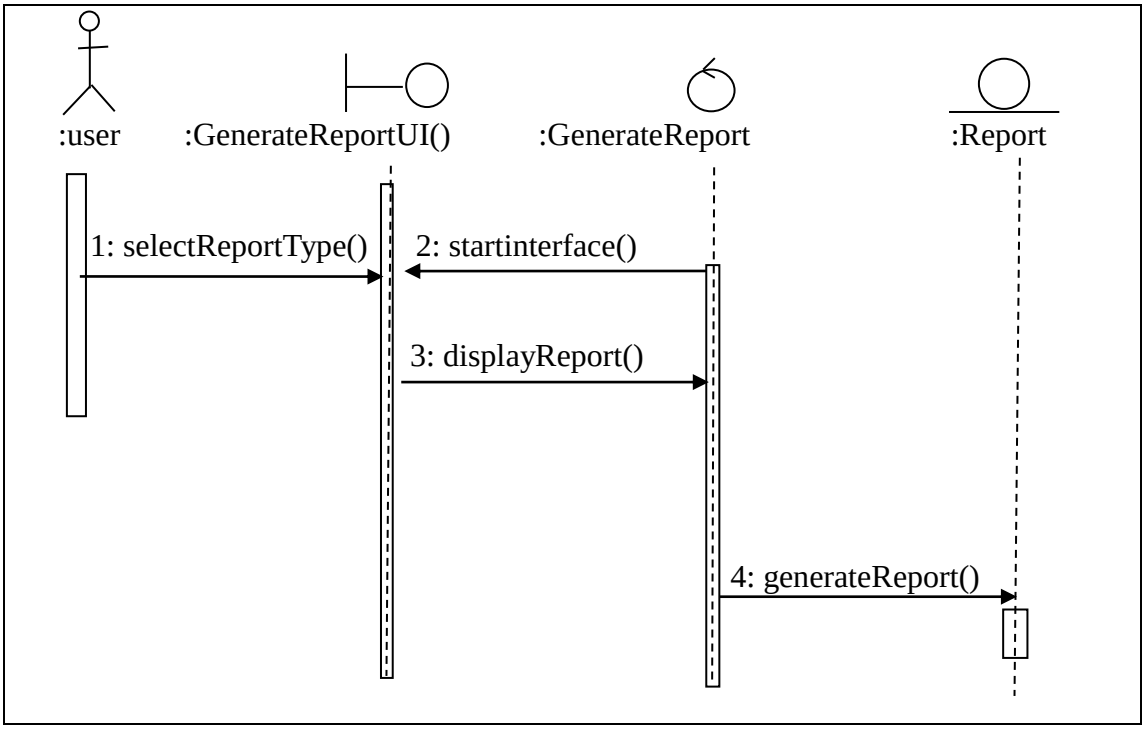


Fig. 34: Generate report sequence diagram

Create User

In Fig. 35, the User Interface is started and then the control object is instantiated. The systems administrator enters user details and then the control object executes the

create user account transaction. The control object then asks the systems administrator to create a user account. The control object finally asks the boundary object to display a message that an account has been successfully created.

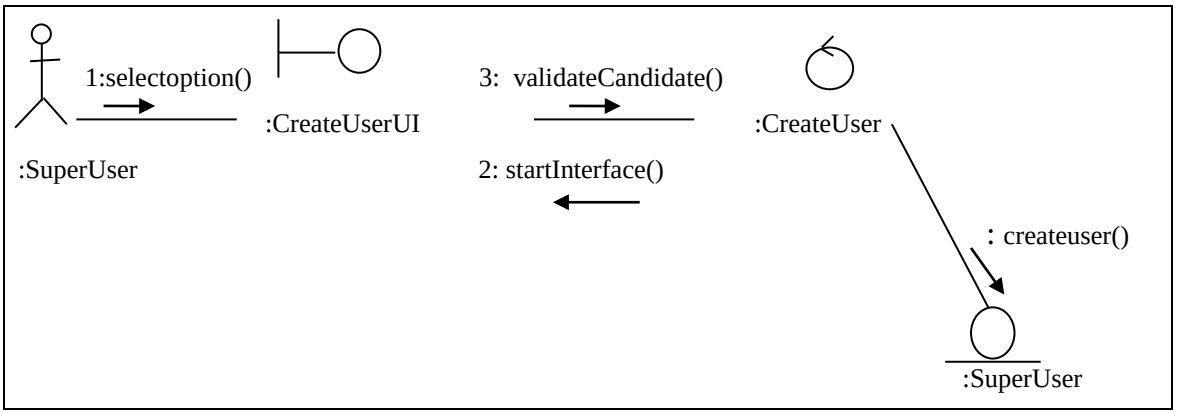


Fig. 35: Create User communication diagram

The sequence diagram in Fig.36 is a synchronization of the communication diagram in Fig.35. The sequence of events for the Generate Report use case is shown in Fig.36.

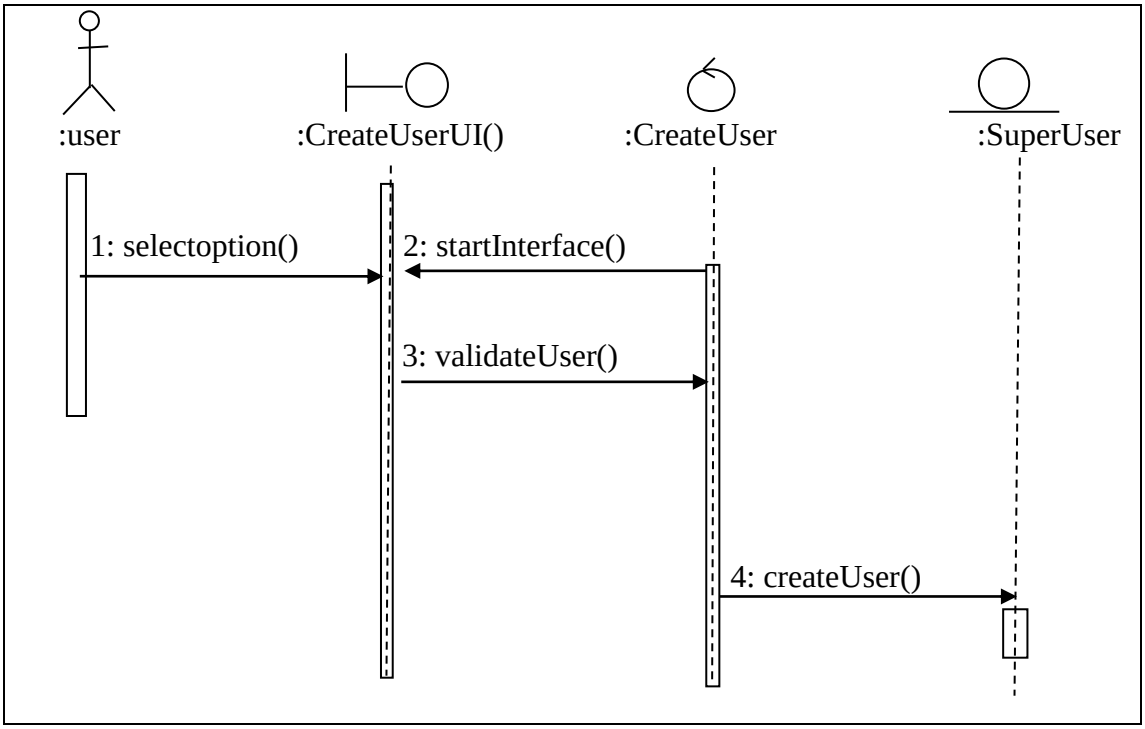


Fig. 36: Create user sequence diagram

Update User

In Fig.37, the user interface is started and then the control object is instantiated. The control object gets the user records from the user account entity object. The use selects the user account they want to update, edit the details and then the control object executes the update user account transaction. The control object then asks the system administrator to update the user record.

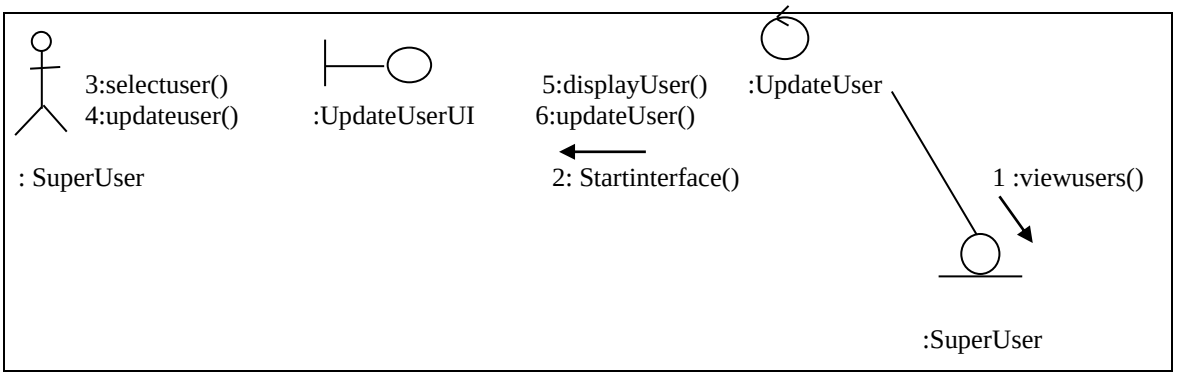


Fig. 37: Update user communication diagram

The sequence diagram in Fig.38 is a synchronization of the communication diagram in Fig.37. The sequence of events for the Update User Account use case is shown in Fig.38.

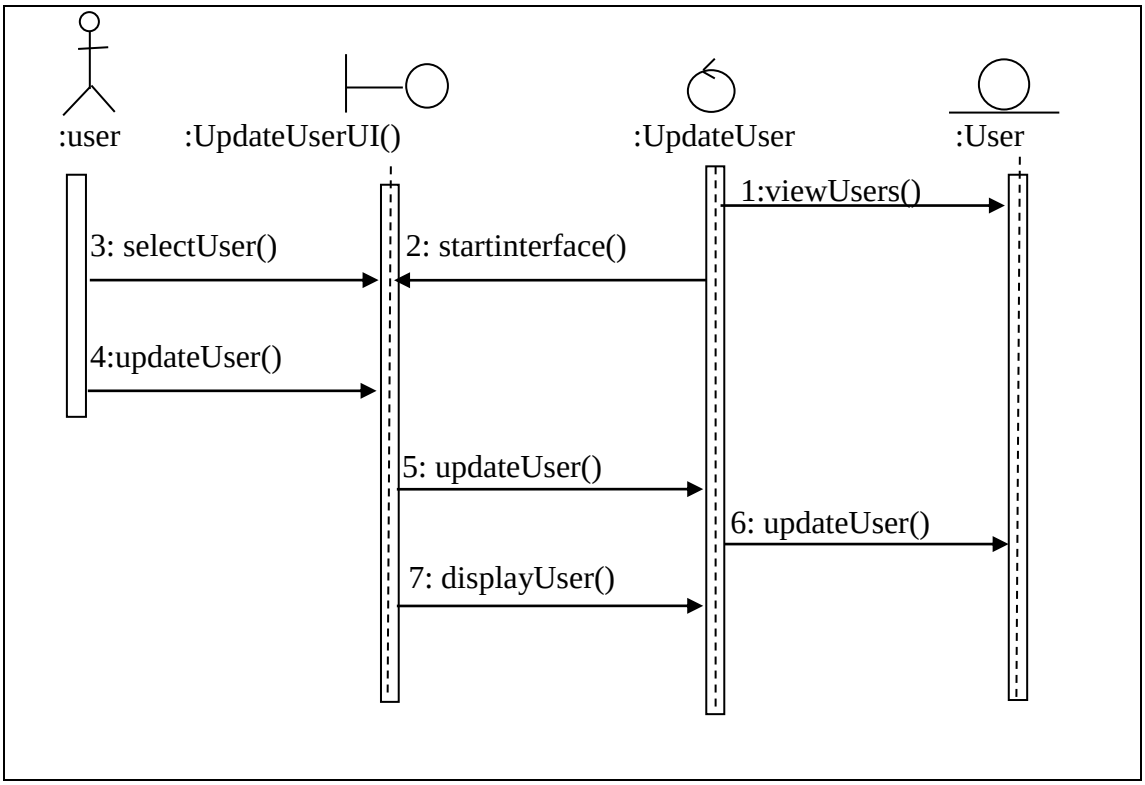


Fig. 38: Update user sequence diagram

Delete User

In Fig.39, the user interface is started and the control object is instantiated. The control object gets the user records from the database from the user account entity. The user selects the record they want to delete, then the control object executes delete user account transaction. The control object then asks the user to delete a user account and finally asks the boundary object to remove the user account record.

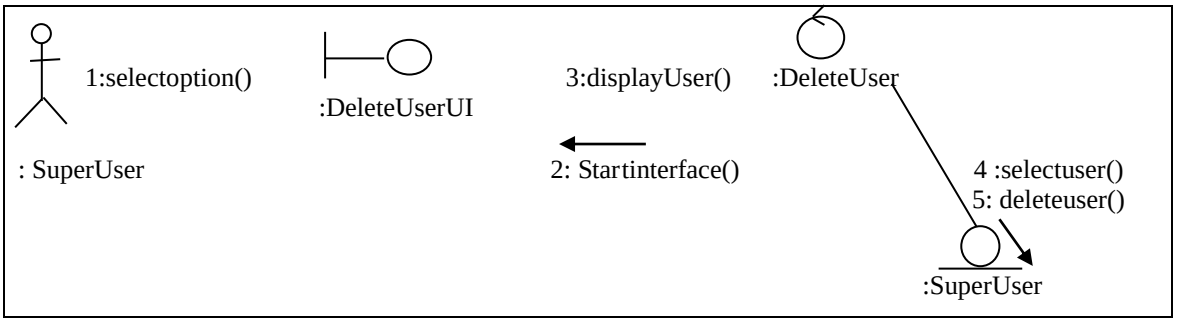


Fig. 39: Delete user account communication diagram

The sequence diagram in Fig.40 is a synchronization of the communication diagram in Fig.39. The sequence of events for the Delete User Account use case is shown in Fig.40.

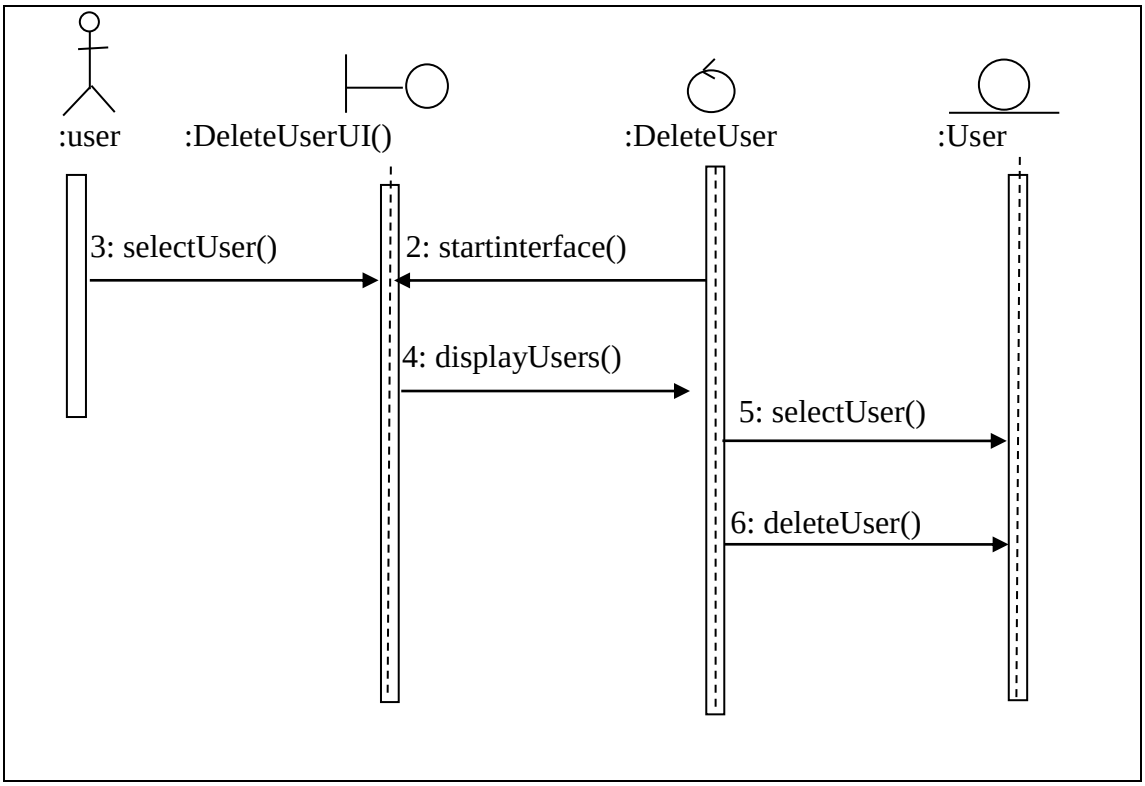


Fig. 40: Delete user sequence diagram

Entity Relationship Diagram

Entity relationship model describes data as entities, attributes and relationships. Figure 41 shows the entity relationship diagram drawn from requirements through interviews and documents such as student registration and examination entry forms.

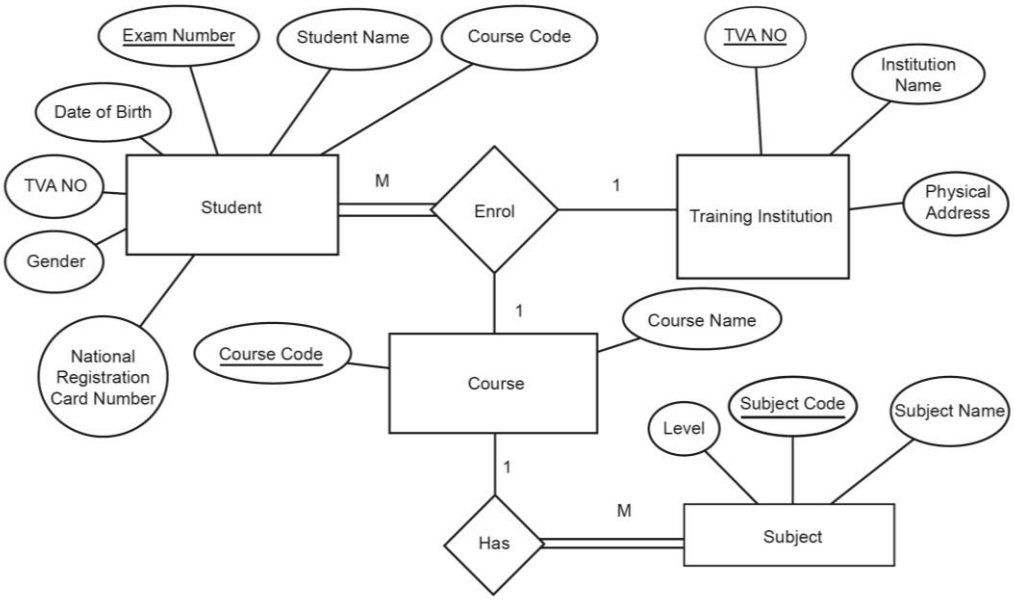


Fig. 41. Entity Relationship Diagram

The entities and attributes that constituted the web and mobile examination results dissemination and verification system are tabulated in tables 8 and table 9.

Table 8 TEVETA examination results dissemination and verification entities and attributes for relational database schema A.

ENTITY : tevetainstitution		
DESCRIPTION : This entity stores data about TEVETA registered institutions		
Attribute	**Description**	**Data Type & Size**
Tvno (Primary Key)	Unique identifier for TEVETA registered institution	VARCHAR(10)
institutionname	Name of institution	VARCHAR(50)
physicaladdress	Physical address of the institution	VARCHAR(50)
Province	Name of province where institution reside	VARCHAR(30)
postaladdress	Postal address for the institution	VARCHAR(50)

ENTITY : Programme		
DESCRIPTION : This entity stores data about programmes candidates register to write examinations		
Attribute	**Description**	**Data Type & Size**
progammename	Unique name for a programme	VARCHAR(50)
Duration	Duration of the programme	CHAR(3)
modeofstudy	Whether the programme is offered on full time, part-time, distance	VARCHAR(30)
ENTITY : Subject		
DESCRIPTION: This entity stores data about subjects (courses in a particular programme)		
Attribute	**Description**	**Data Type**
Subjectcode (Primary Key)	Unique identifier for a subject	VARCHAR(10)
programmename	Unique name of the programme	VARCHAR(50)
subjectname	Name of the subject	VARCHAR(50)
Level	Level for each coursecode	VARCHAR(3)
ENTITY : Student		
DESCRIPTION: This entity stores data about candidates		
Attribute	**Description**	**Data Type**
Examnumber (Primary Key)	Unique identifier for candidate	INT(11)
password	Candidate's password	VARCHAR(100)
institutionname	Examination centre name	VARCHAR(50)
programmename	Candidate's programme study	VARCHAR(100)
Level		
year_of_enrolment	Year when candidate first registered	INT(11)
Firstname	Candidate's forename	VARCHAR(50)
lastname	Candidate's lastname	VARCHAR(50)
othername	Candidate's maiden name	VARCHAR(50)
Gender	Candidate's sex	CHAR(1)
nrcnumber	Candidate's national registration card number (mandatory for Zambian citizens)	VARCHAR(11)
passport	Candidate's passport number (mandatory for Non-Zambians	VARCHAR(50)

ENTITY: Results		
DESCRIPTION: This entity stores students' examination results		
Attribute	**Description**	**Data Type**
Serialnumber (Primary Key)	Unique identifier for each record	INT(11)
Studentnumber	Unique identifier for candidate	INT(11)
Coursecode	Unique identifier for each subject (coursename)	VARCHAR(6)
Mark	Encrypted mark for each mark according to coursecode	VARCHAR(250)
Grade	Classification of a mark obtained by candidate	CHAR(1)
Level	Candidate level in a particular programme of study: e.g. Level 1,II or III	VARCHAR(3)
Year	Year of examination	INT(11)

Table 9 TEVETA examination results dissemination and verification entities and attributes for relational database schema B.

ENTITY : hashedmarks		
DESCRIPTION: This entity stores hashed marks of students		
Attribute	**Description**	**Data Type**
Serialnumber	Unique identifier for each record	INT(11)
Studentnumber	Unique identifier for candidate	INT(11)
Coursecode	Unique identifier for each subject (coursename)	VARCHAR(10)
Mark	Hashed mark for each mark according coursecode	VARCHAR(250)
Level	Candidate level in a particular programme of study: e.g. Level 1,II or III	VARCHAR(3)
Year	Year of examination	INT(11)

In table 10 and table 11, the Relational schemas for TEVETA web and mobile based examination results dissemination system are presented.

Table 10 TEVETA examination results dissemination and verification relational database schema A.

tevetainstitution (tvno, institutioname, physicaladdress, province, postaladdress)
programme (programmename, duration, modeofstudy)
subject (subjectcode, programmename, subjectname, level)
Student (examnumber, institution name, programmename, level, year_of_enrolment, firstname, lastname, othername, gender, nrcnumber, passport)
Results
results (serialnumber, examnumber, coursecode, mark, grade, level, year)

Table 11 TEVETA examination results dissemination and verification relational database schema B.

hashedmarks (serialnumber, examnumber, coursecode, mark, level, year)

3.4 System Implementation

In this study, most development tools used were open source as they are available at no cost. The open source development tools used were Apache web server, MYSQL and Hypertext Preprocessor (PHP). Proprietary software, Adobe Dreamweaver text editor was used; Hyper Text Markup Language (HTML) was used for creating web pages, Cascading Style Sheet (CSS) was used for styling web pages and JavaScript was used for making web pages interactive.

The proposed system has two components; Web and Short Message Service/Unstructured Supplementary Service Data (SMS/USSD) application. The web and mobile applications were developed using Hypertext Preprocessor (PHP) and Java programming languages respectively. Both applications used AES encryption algorithm integrated with SHA3-224 cryptographic hash function to provide cyber security objectives of confidentiality, integrity and authenticity assurances on students' examination results. The web application allows authorised users to use a computer, tablet or smart phones with internet connection to register a candidate for examination, examination results entry and retrieval. The mobile application allows

students to send requests to MYSQL database in order to view both examination enrolment details and examination results using a mobile phone.

3.4.1 Secure insertion and storage of marks

During insertion of examination results, each plain text mark is simultaneously encrypted with AES encryption algorithm and hashed with SHA3-224 hashing algorithm. The final encoded mark consists of two parts. One part of the encoded mark is the encrypted mark and the other is a hashed mark. The hashed mark and encrypted mark are saved in independent databases. The hashed mark is used to check the integrity of the stored encrypted marks during retrieval of examination results. Figure 7 in section 3.3.3 shows the architecture for secure insertion and storage of examination results. The algorithm for secure insertion and storage of examination results using AES encryption and SHA3-224 is given in section 3.3.4. Table 12 and 13 is PHP snippet of code for secure insertion of marks using SHA3-224 cryptographic hash function and AES encryption algorithm.

Table 12 PHP snippet of code for secure insertion of examination results using SHA3-224 hashing algorithm

```
$hashmark[$i]=hash('SHA3-224',$mark[$i]);
$queries = array();
$queries[]="('$serialnumber[$i]','$studentid[$i]','$coursecode[$i]','$hashmark[$i]','$level[$i]','$year[$i]')";
$insert="INSERT INTO hashedmarks(serialnumber, studentnumber, coursecode,mark, level, year)VALUES $values";
```

Table 13 PHP snippet of code for secure insertion of examination results using AES Encryption algorithm

```
$update= mysqli_query($link, "UPDATE TEST SET studentnumber= '$studentid[$i]',coursecode='$coursecode[$i]',mark=AES_ENCRYPT('$mark[$i]','$key'),grade='$grade[$i]',level='$level[$i]',year='$year[$i]'where serialnumber='$serialnumber[$i]'");
```

3.4.2 Secure retrieval of examination results

During retrieval of student marks, SHA3-224 is used to check the integrity of each stored encrypted mark to ensure that the mark was not altered in transit or in the database. The process involves comparing the hash of the decrypted mark with its equivalent hashed mark originally stored in database (b). If the hashes of marks match, the AES algorithm will proceed to display decrypted marks, otherwise it will return an alert as it is an indication that marks were altered while in transit or storage and therefore are not authentic. Figure 8 in section 3.3.3 shows the architecture for secure retrieval of examination results. The algorithm for secure retrieval examination results using AES encryption and SHA3-224 is given in section 3.3.4. The snippet code for secure retrieval of examination results is given in table 14.

Table 14 snippet of code for retrieval of examination results using AES encryption algorithm and SHA3-224 hashing algorithm

```
$select="SELECT AES_DECRYPT(mark,'$key') FROM results WHERE studentnumber='$studentnumber'";
$result = mysqli_query($link, $select);
while($row = mysqli_fetch_assoc($result)){
$mark = $row["AES_DECRYPT(mark,'$key')"];
$hashmark=hash('sha3-224',$mark);
$query1 ="SELECT mark FROM hashedmarks WHERE mark='$hashmark'";
$check = mysqli_query($link2,$query1);
if(mysqli_num_rows($check)= =0) {
echo "Could not retrieve your results. Please check with TEVETA";
exit();
/* retrieve results */
}
else {$result = mysqli_query($link, "SELECT results.studentnumber, results.coursecode, results.grade, results.level, results.year FROM results, studentdetails where studentdetails.studentnumber=results.studentnumber AND results.studentnumber='$studentnumber'");
}
```

3.5 Summary

This chapter discussed the materials and methods used in the baseline study, the system design and the architecture for secure storage and dissemination of examination results. A mixed methods methodology was used in this study. Purposeful sampling was used in the selection of the sample size for the baseline study. The current business processes for candidate registration and dissemination of examination results were analysed and proposed business process models for secure storage and dissemination of examination results were presented.

CHAPTER FOUR
RESULTS

4.1 Introduction

This chapter presents the results derived from the baseline line study. The objective of the baseline study was to establish the challenges faced by TEVETA and students regarding dissemination of examination results. Results from the prototype are also presented in this chapter.

4.2 Baseline Study

In this section, results from the baseline study are presented. The results are presented in form of bar charts, pie charts and tables.

4.2.1 Demographic Information

Data was collected from 558 respondents consisting of 514 students, 36 members of staff in-charge of examinations in institutions of study and 8 TEVETA ICT staff. The 514 students and 36 members of staff in charge of examinations were from 12 TEVETA registered institutions country wide.

4.2.1.1 Distribution of respondents by Occupation

Respondents were grouped by their occupation: 92 percent were students, 7 percent were members of staff in charge of examinations from various training institutions, and 1 percent were IT staff from TEVETA. The occupation of TEVETA respondents was critical in establishing the different level of involvements of various people in candidate registration, examination results entry and management of TEVETA Information Systems. Examination candidates (students) were also involved because they are affected by problems in registration for examinations and delays in the

release of examination results. Figure 42 shows the distribution of respondents by occupation.

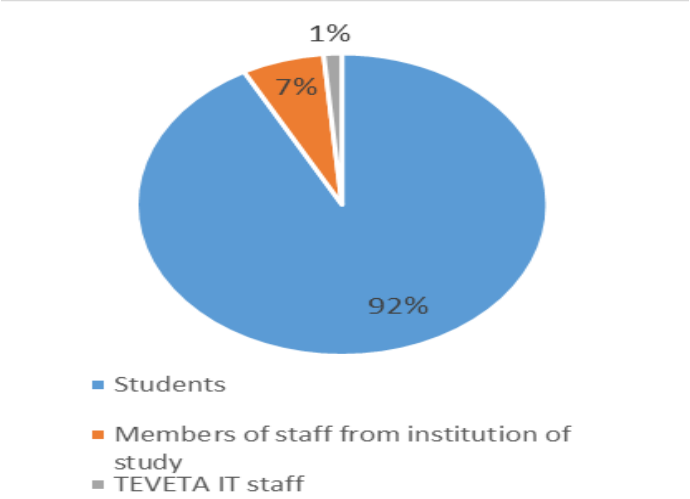


Fig.42: Distribution of respondents by occupation

4.2.1.2 Distribution of students by programme of study

Figure 43 show that out of 514 students who participated in the study, 45 percent were studying a Diploma programme, 33 percent were studying a Trade Certificate programme and 22 percent were studying a Craft Certificate programme. All students from various programmes of study were considered during research as TEVETA offers Trade Certificate, Craft Certificate and Diploma programmes.

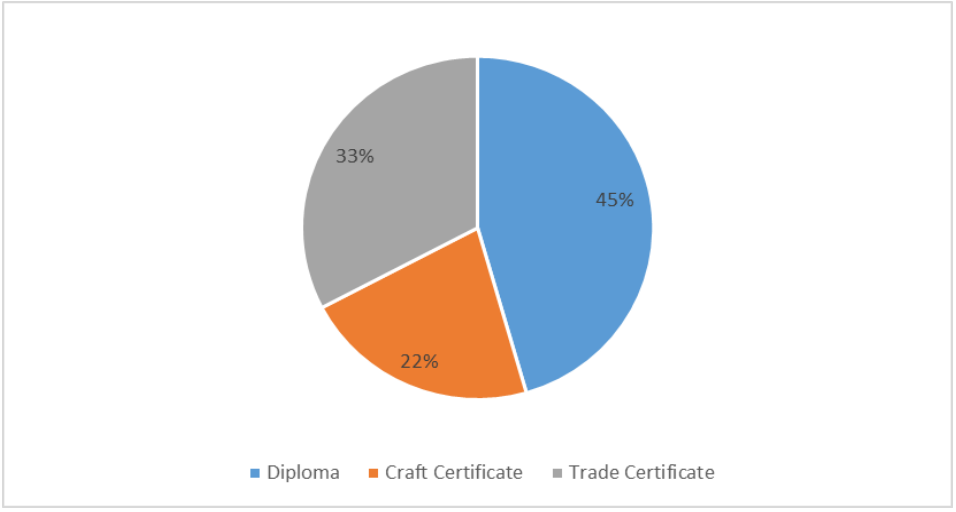


Fig. 43: Students' programme of study

4.2.1.3 Category of Institution

Figure 44 show that 42 percent were Colleges, 33 percent were Training Centers and 25 percent were Trade Schools. The category of institution was important because TEVETA has three categories of institutions: Colleges, Training Centers and Trade schools. In this study, all categories of institutions were considered.

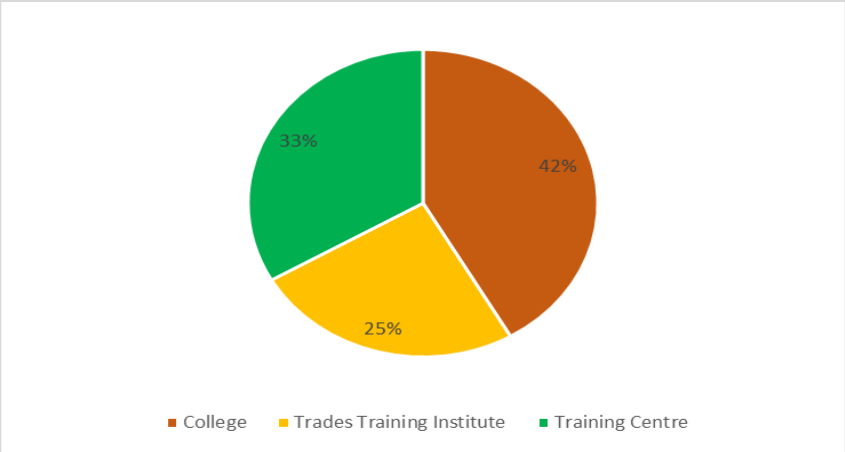


Fig. 44: Category of institutions

4.2.2 Challenges with the current candidate registration and examination results dissemination system

This section addresses objective number one which was to establish the challenges faced by TEVETA and students regarding dissemination of examination results. The research started by finding out if members of staff from institutions of study and TEVETA face challenges with the current candidate registration processes and dissemination of results. The results of the findings are presented using charts.

4.2.2.1 Challenges faced by staff in charge of examination in institutions of study

Questionnaires were administered to 36 members of staff in charge of examination in institutions of study. The research finding reveal that a number of challenges were faced in candidate registration for examinations. As indicated in Fig.45, the

respondents mentioned challenges such as registration forms received late which accounted for 2 percent, disparities in the number of students registered for examination between institutions of study and TEVETA accounted for 11 percent, 5 percent said incorrect examination numbers resulting into duplicate entries, 3 percent said incorrect subject entries, failure by students to verify their details accounted for 5 percent, incomplete registration forms accounted for 9 percent, non-submission of registration forms accounted for 5 percent, forms received late accounted for 9 percent, errors in data entry accounted for 13 percent, large number of students accounted for 6 percent, few personnel in data entry accounted for 11 percent, registration of illegal students accounted for 9 percent, other accounted for 2 percent, omission of candidate registration details sent to TEVETA accounted for 12 percent.

4.2.2.2 Challenges faced by TEVETA IT staff in candidate registration for examinations

Questionnaires were administered to 5 TEVETA Data Entry Personnel responsible for candidate registration and examination results entry. The research findings reveal that the challenges faced are: incomplete registration forms which account for 13 percent, incorrect subject entries by candidates which account for 13 percent, registration forms received late which account for 16 percent, few personnel in data entry accounted for 9 percent, large number of students accounted for 9 percent, incorrect examination numbers entered resulting into duplicate entries accounted for 3 percent, TEVETA application failure to capture all students accounted for 9 percent, disparities in the number of students registered for examinations between the institution of study and TEVETA accounted for 13 percent and failure by students to verify their details accounted for 13 percent. Figure 46 shows challenges faced by TEVETA in candidate registration.

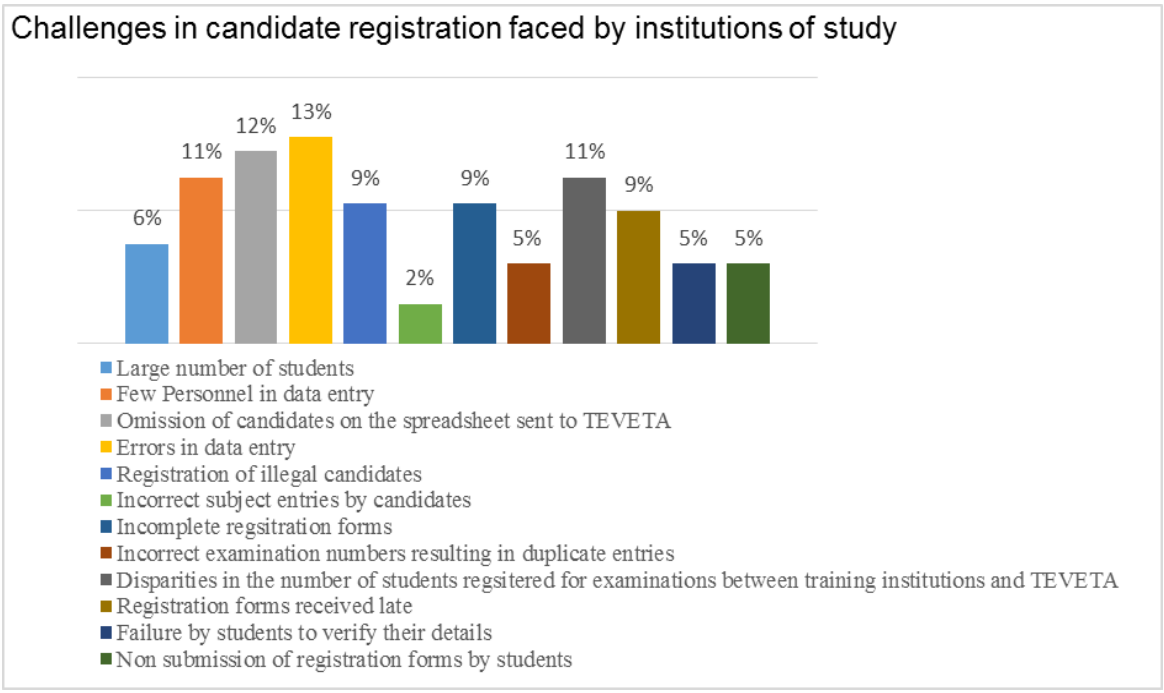


Fig.45: Candidate registration challenges faced by staff in institutions of study

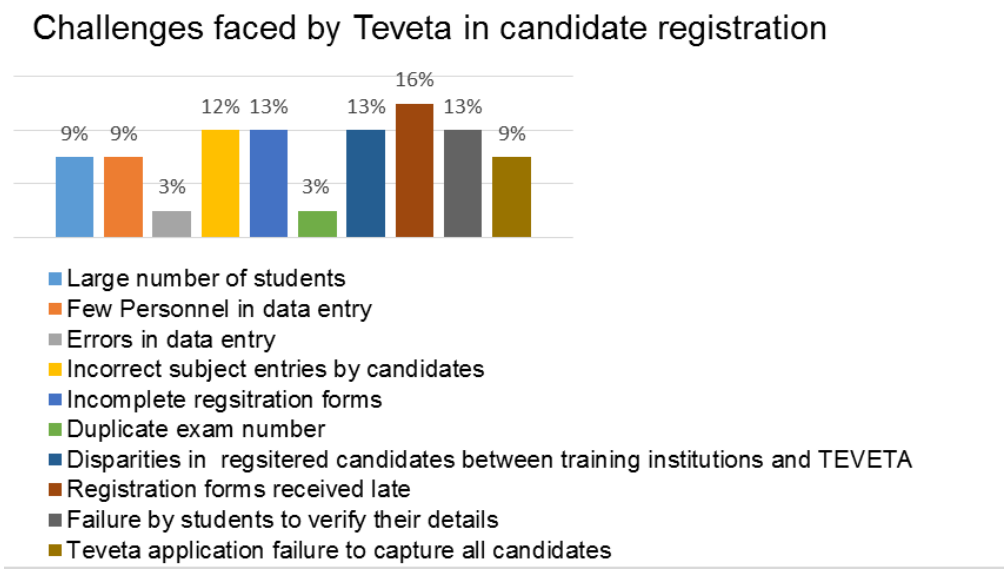


Fig. 46: Challenges faced by TEVETA in candidate registration for examinations

4.2.3 Factors that delay the release the examination results

The research findings from TEVETA IT staff reveal that a number of factors delay the release of examination results. As indicated in Fig.47, the factors that delay the release of TEVETA students' examination results were: long and tedious administrative procedures before the release of examination results which accounted for 33 percent,

large number of students accounted for 25 percent, few personnel accounted for 34 percent, late submission of continuous assessment results by institutions of study accounted for 8 percent.

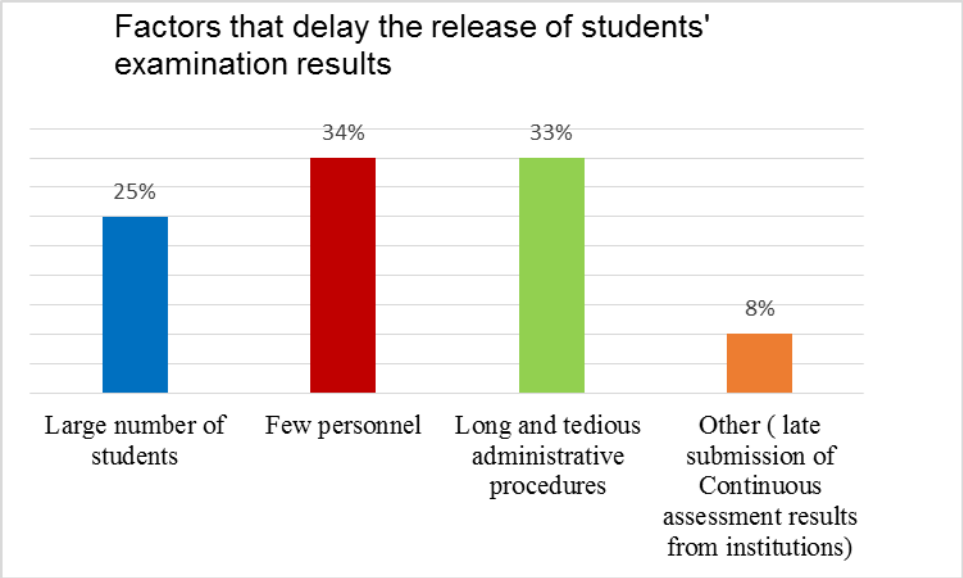


Fig. 47: Factors that delay the release of examination results

The research findings from TEVETA examined students confirm the delay in release of examination results. Out of 514 student respondents, 48 percent said results are released after three months, 32 percent said after two months while 20 percent said it varies. The delay in release of examination results lead to reduction of the first term of the TEVET academic calendar to only a month as students are not allowed to proceed to the next level of study before examination results are released. Figure 48 shows how long it takes for TEVETA to release examination results.

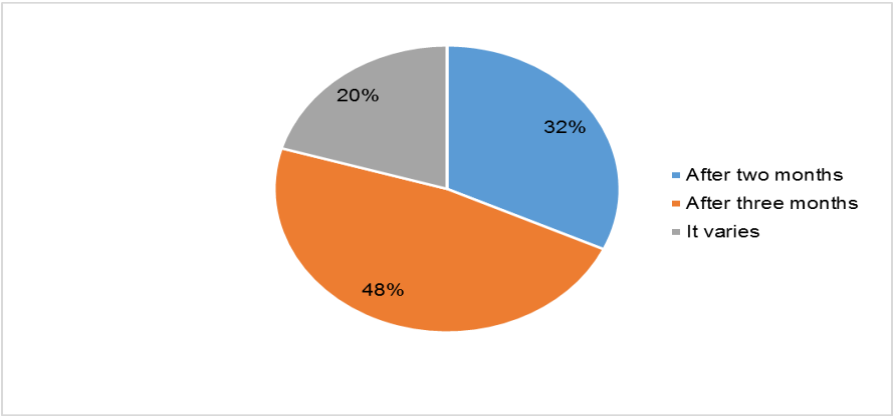


Fig. 48: How long it takes for TEVETA to release results

4.2.4 How long it takes for students to know results after they are released

Having established that they were challenges in the release of examination results, the researcher went on to find out how long it takes for them to know their results. Figure 49 show that 43 percent know their results after some weeks, 43 percent said after some days, 6 percent said within a day and 8 percent after a month.

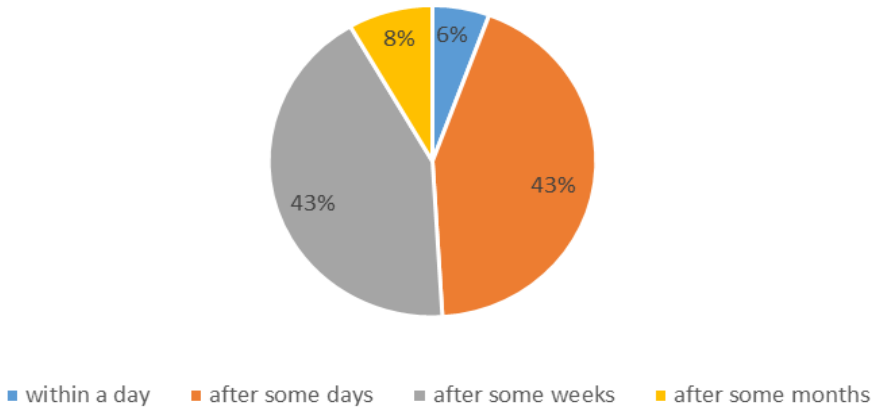


Fig. 49: How long it takes for students to know results after they are released

The baseline study reveals that some institutions of study do not allow their students to proceed to the next level of study as it is a requirement by TEVETA not to allow students to proceed to the next level of study before results are released. Figure 50 show that 83 percent of students are not allowed to proceed to the next level of study while 17 percent are allowed by their institutions of study to proceed to the next level of study before examination results are released.

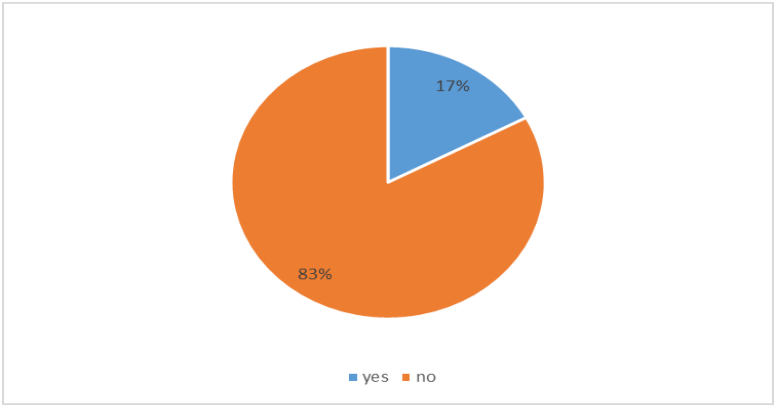


Fig. 50: Whether students are allowed to proceed to the next level of study

The delay in the release of examinations affects syllabi coverage as shown in Fig.51. This is because 86 percent of students said their institutions of study do not put in measure to ensure that they cover the whole syllabi while 14 percent said their institutions of study do.

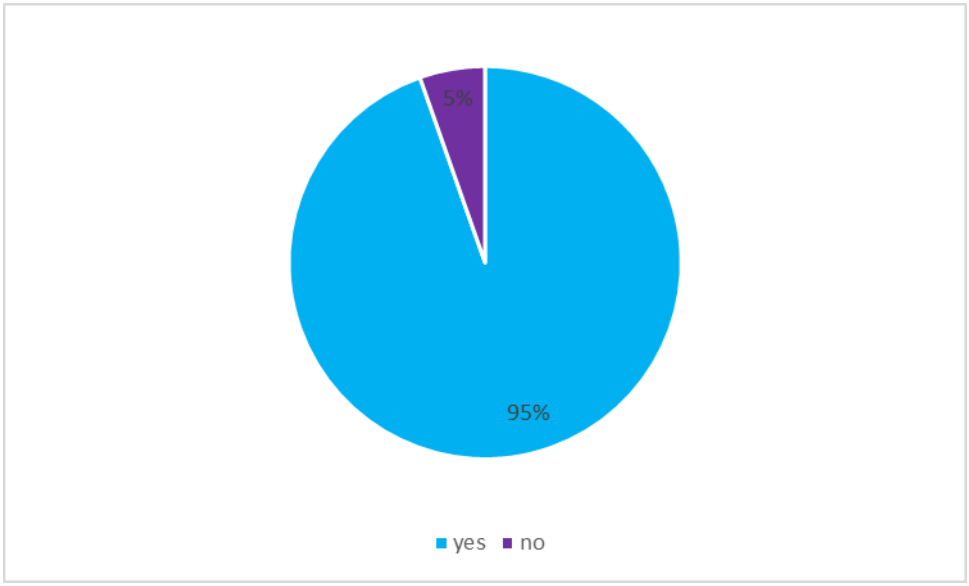


Fig. 51: Whether the delay in releasing results affects syllabi coverage

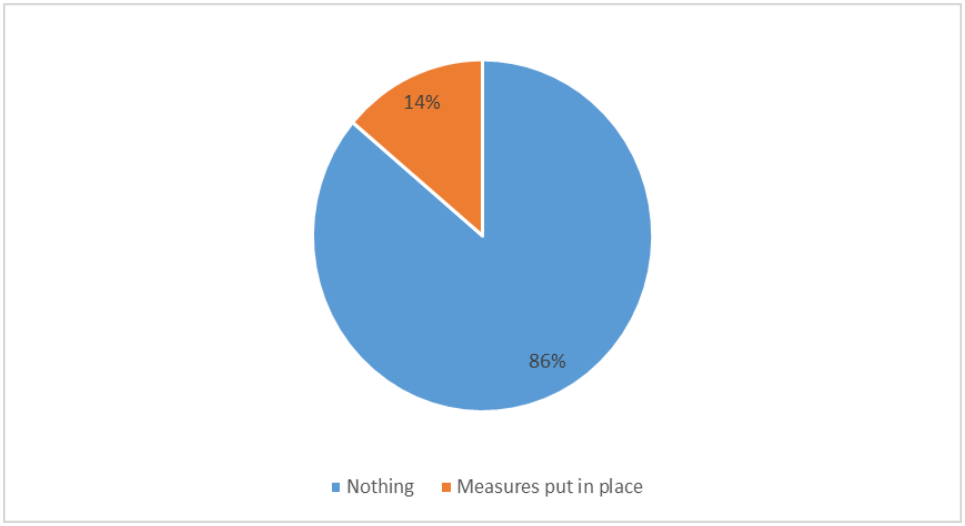


Fig. 52: Whether measures are put in place to finish the syllabi

4.2.5 Suggested Solutions by Respondents

Having established the challenges, respondents from TEVETA, members of staff in charge of candidate registration in institutions of study and students were asked to recommend solutions that would help in reducing or eradicating some of the

challenges. They all recommended a web based application for candidate registration and that candidate registration for examinations should be done directly by institutions of study so as to eliminate redundancy of effort. This is because currently candidate registration for examination is done from both the institution of study and TEVETA. They further recommended a mobile and web application for dissemination of students' examination results.

4.2.5.1 Suggested solutions by TEVETA examined students

As shown in Fi.53, 76 percent of students said a mobile application would improve access to examination results, 21 percent are not sure while 3 percent said a mobile application cannot improve access to results. Further, the study revealed that 96 percent of students have mobile phones while 4 percent do not have as shown in Fig. 54.

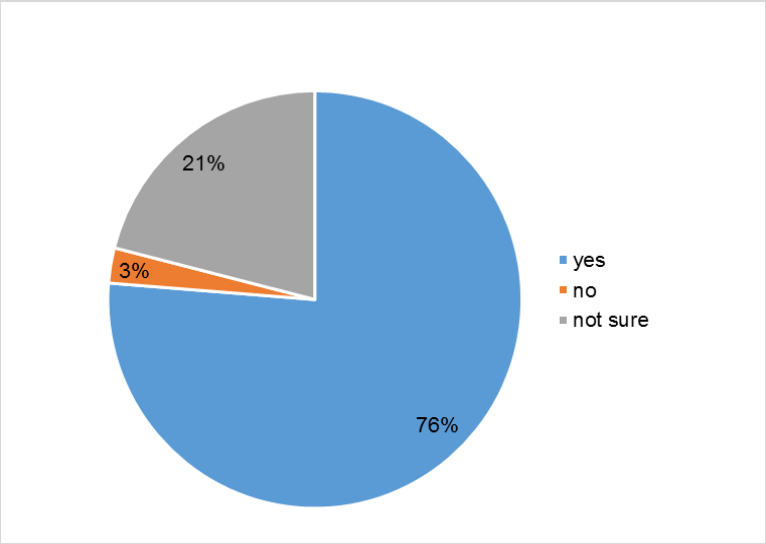


Fig.53: Whether a mobile application would improve access to examination results

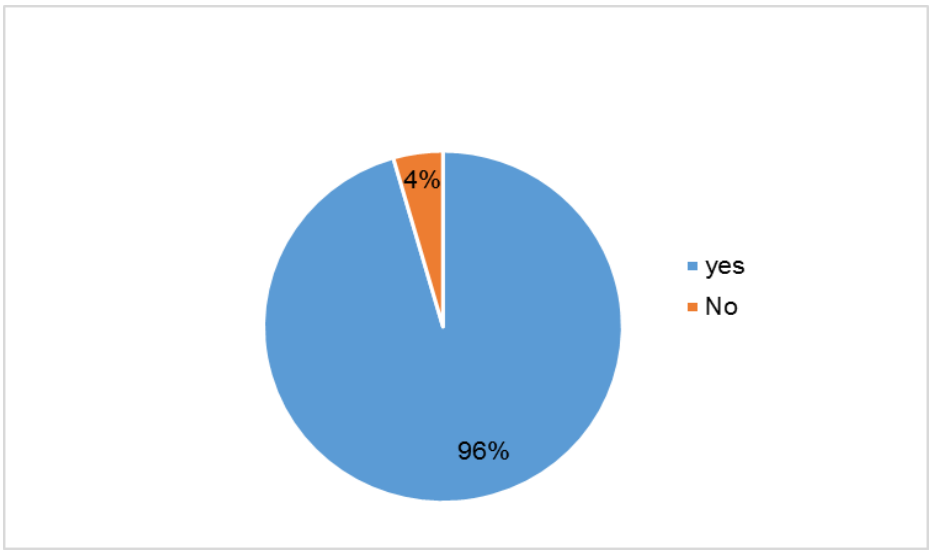


Fig. 54: Students with mobile phones

The student participants also indicated the mobile network providers available in their area. According to Fig.55, at least one mobile network provider is available in their area making it possible for them to use mobile phones to access examination results.

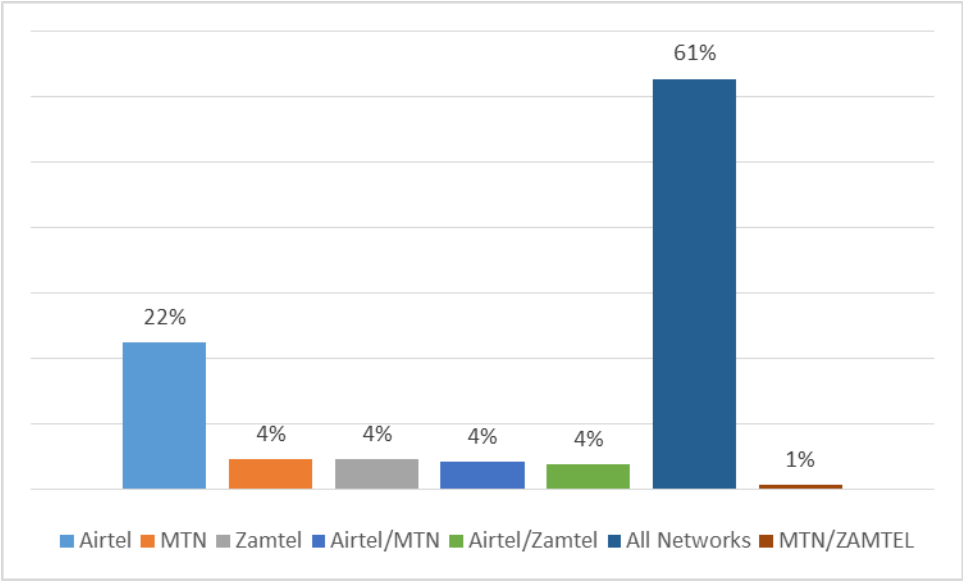


Fig.55: Students' responses on mobile network provider available

Figure 56 shows that 71 percent of students agreed that a web application can improve efficiency in dissemination of examination results, 3 percent disagreed while 26 percent said they were not sure.

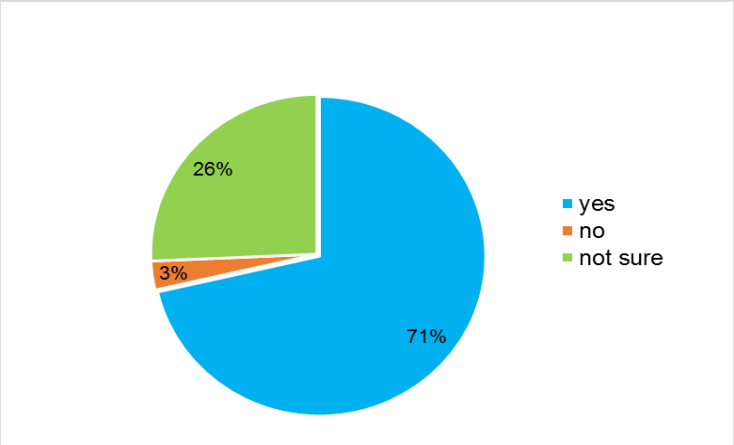


Fig. 56: Students' responses on whether a web application would improve access to results

Students were asked if they have access to the internet. Figure 57 shows that 82 percent have access to internet while 18 percent do not have access to the internet.

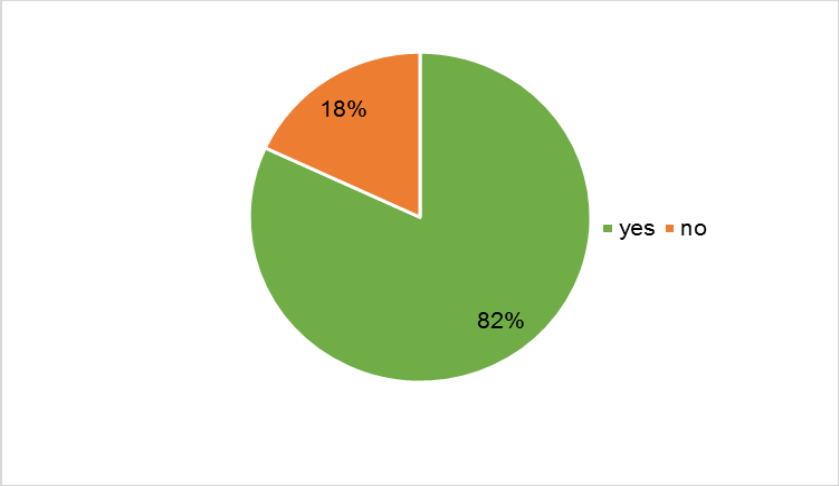


Fig. 57: Students' access to internet

According to Fig.58, 57 percent of students access internet through mobile devices, 17 percent through their institution of study, 5 percent access the internet through the internet café, 1 percent access through public Wi-Fi only and 18 percent through a combination of more than one method.

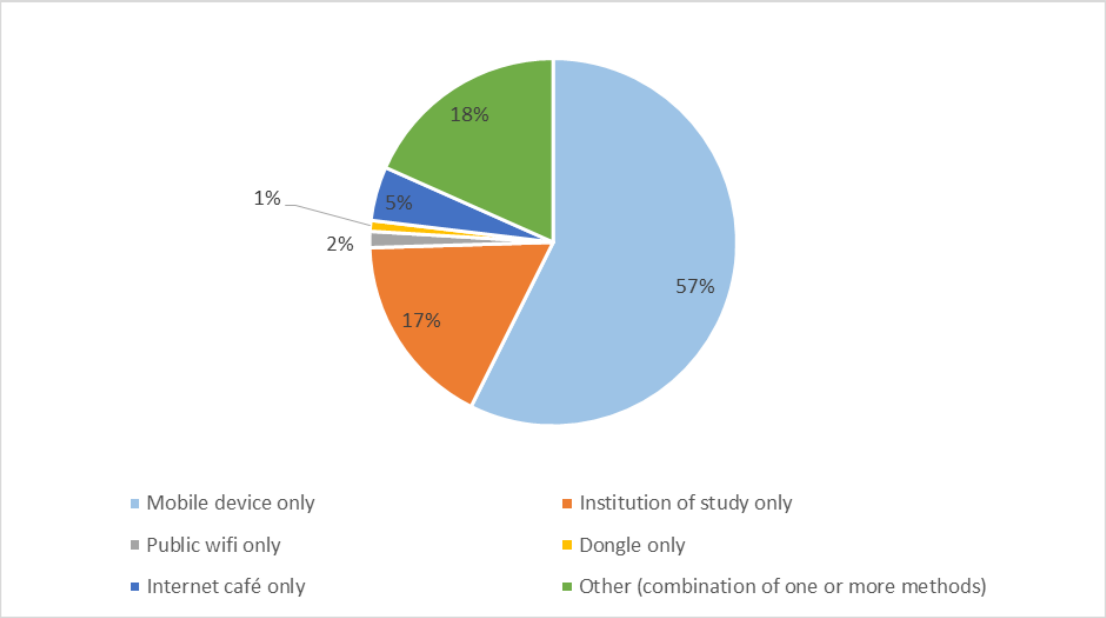


Fig. 58: Ways students access the internet

4.2.5.2 Suggested solutions by TEVETA Data Entry Personnel

All TEVETA data entry personnel respondents recommended that a mobile and web based application would improve dissemination of examination results. TEVETA data entry personnel were asked to recommend features in a mobile application for dissemination of examination results and the responses as shown in Fig.59 were as follows: allow candidates to enrol for examinations using a mobile phone accounted for 10 percent , allow candidates to verify their details accounted for 13 percent, allow candidates to view their details accounted for 11 percent, detect illegal candidates accounted for 10 percent, eradicate wrong subject entries by candidates accounted for 13 percent, eradicate multiple registrations by the same candidate accounted for 11 percent, secure storage of candidate enrolment and examination results accounted for 11 percent, allow students to view examination results accounted for 11 percent and other (allow students to view results for a specified period) accounted for 8 percent.

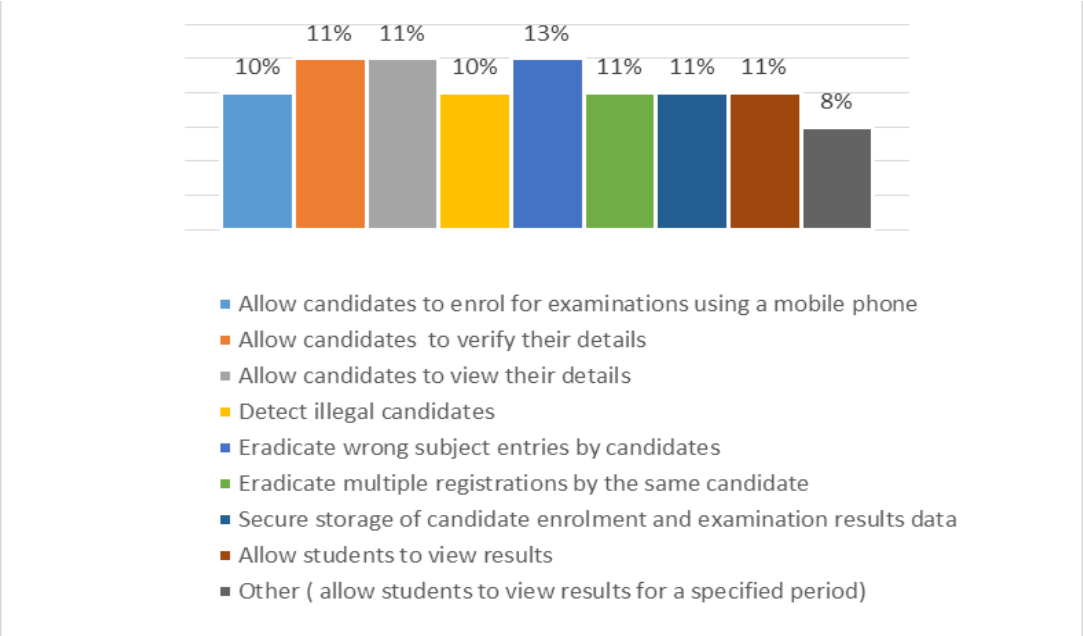


Fig. 59: Features commended by TEVETA in a mobile application

Further, TEVETA data entry personnel were asked to recommend features in a web application for dissemination of examination results and the responses as shown in Fig.60 were as follows: allow candidates to enrol for examinations online accounted for 10 percent, allow candidates to view enrolment details accounted for 8 percent, eradicate wrong subject entries by candidates accounted for 8 percent, eradicate multiple registrations by same candidate accounted for 8 percent, allow candidates to verify their details online accounted for 12 percent, detect illegal candidates accounted for 10 percent, allow students to view enrolment details accounted for 12 percent, deter unauthorised amendments to examination results accounted for 10 percent, secure storage of candidate enrolment and examination results accounted for 10 percent, allow students to view examination results accounted for 10 percent and other (allow students to view for a specified period) accounted for 8 percent.

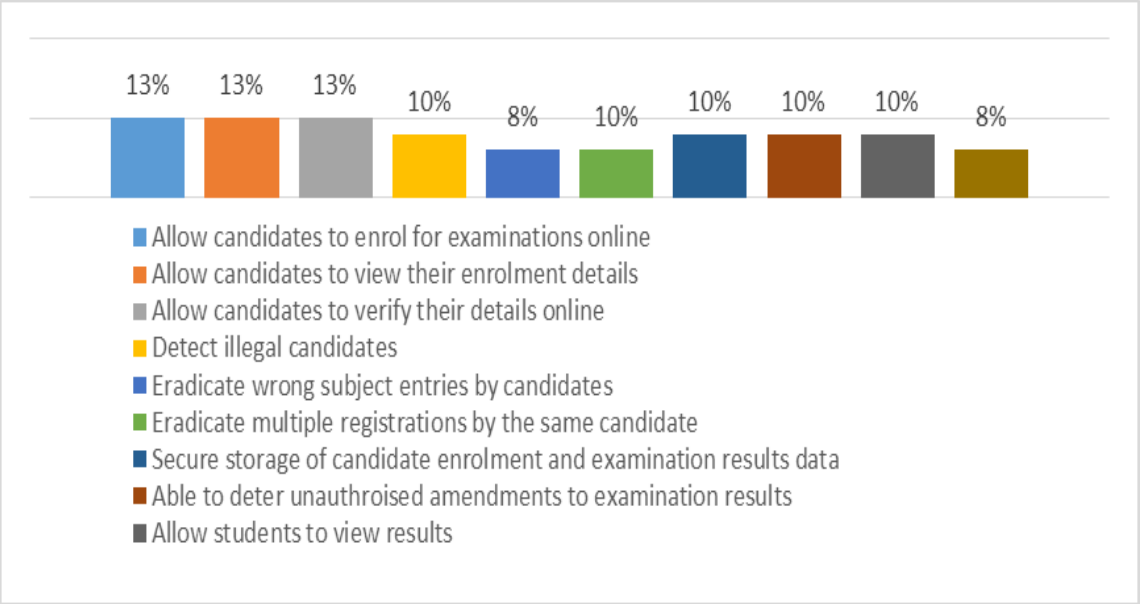


Fig.60: Features commended in a web application by TEVETA

4.2.5.3 Solutions recommended by members of staff in charge of examinations in institutions of study

Members of staff from institutions of study in charge of examinations were asked to recommend features in a mobile application for candidate registration and dissemination of examination results and their responses as shown in Fig.61 were: allow candidates to enrol for examinations using a mobile phone accounted for 14 percent, allow candidates to verify their details accounted for 17 percent, allow candidates to view their details accounted for 17 percent, reject illegal candidates accounted for 17 percent, eradicate wrong subject entries by candidates accounted for 13percent and reject multiple registrations by the same candidate accounted for 17 percent.

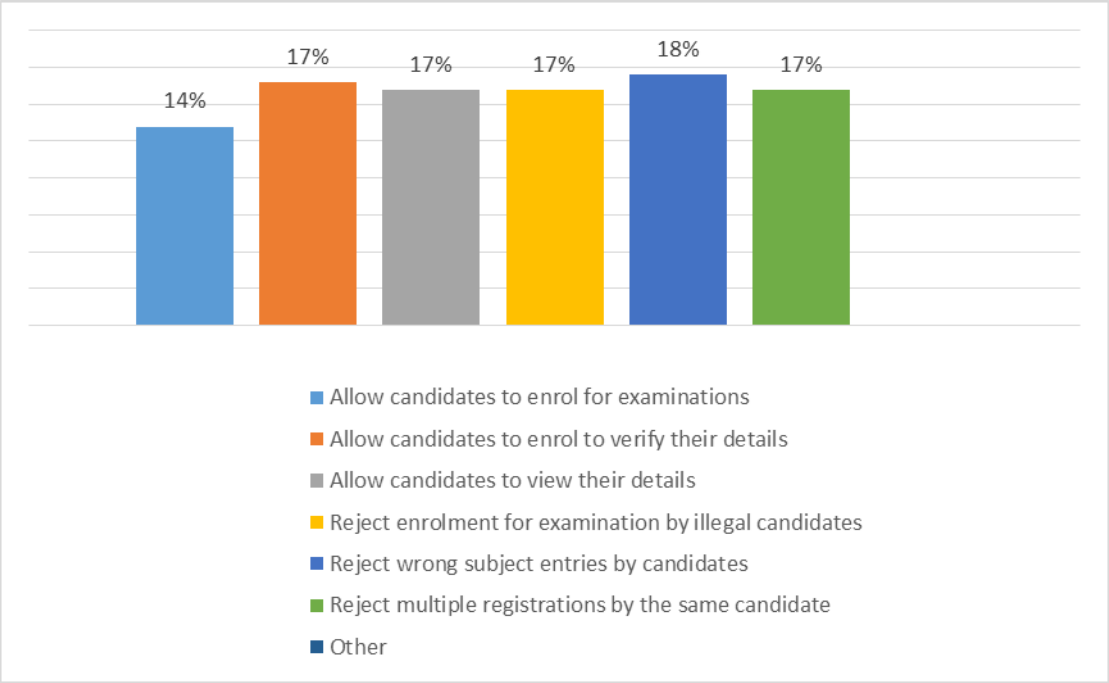


Fig.61: Features commended in a mobile application by staff in institutions of study

Further, members of staff from various institutions of study were asked to recommend features in a web application for registration and dissemination of examination results and the responses as shown in Fig.62 were as follows: allow candidates to enrol for examinations online accounted for 18 percent, allow candidates to view enrolment details accounted for 17 percent, eradicate wrong subject entries by candidates accounted for 16 percent, eradicate multiple registrations by same candidate accounted for 16 percent, allow candidates to verify their details online accounted for 17 percent, detect illegal candidates accounted for 16 percent. Further, some staff in TEVETA registered institutions recommended that TEVETA should develop a web application that can allow members of staff in charge of candidate registration in institutions of study to register students online to curb extensive use of paper and avoid registration of candidates from both the institution of studies and TEVETA.

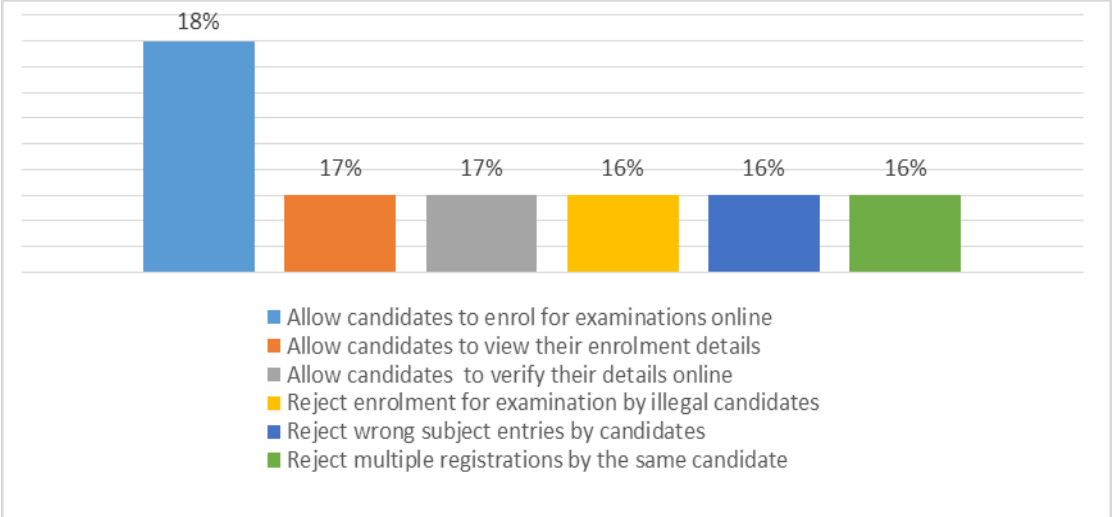


Fig. 62: Features commended in a web application by staff in institutions of study

4.2.6 Challenges with the current payment system for fees

The research further revealed that some students face problems with the current TEVETA payment system for registration and examination fees as shown in Fig.63.

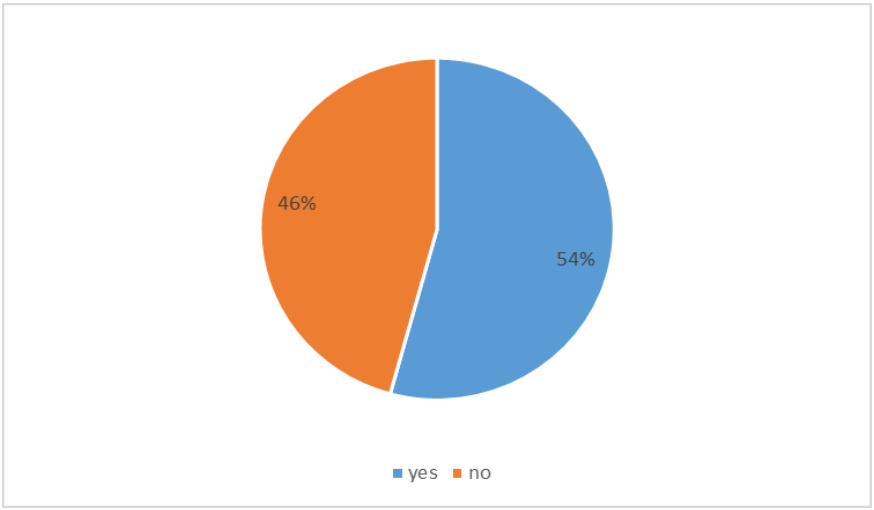


Fig. 63: Whether students face challenges with the current payment system for fees

After establishing that indeed there were challenges, students were asked what these challenges were. The challenges mentioned by students are shown in Fig.64.

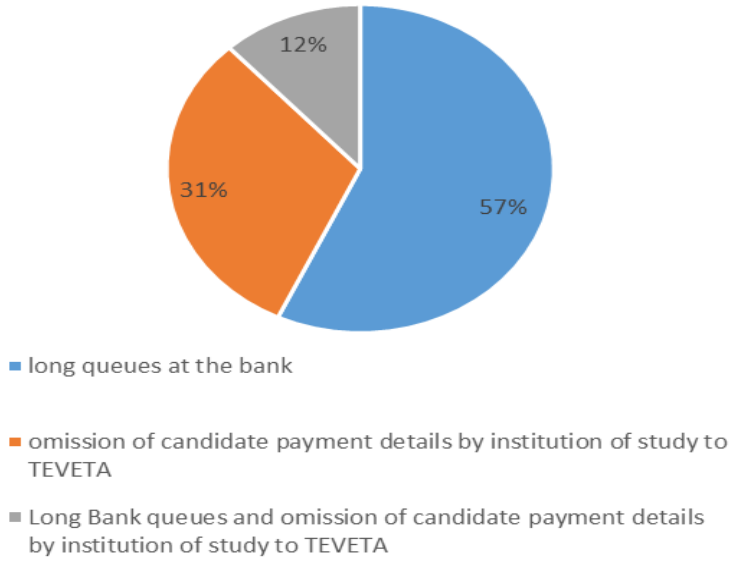


Fig.64: Problems faced with current payment system for fees

4.2.6.1 Students with bank accounts

As shown in Fig.65, 54 percent of students have bank accounts while 46 percent do not have. Further, the study showed the following: 6 percent of students have accounts with Barclays Bank, 13 percent have accounts with First National Bank, 56 percent have accounts with Zambia National Commercial Bank, 4 percent have accounts with Stanbic bank, 4 percent have accounts with standard Chartered Bank, 11 percent have accounts with Atlasmara, 5 percent have accounts with Indo Zambia Bank, 1 percent have accounts with ECO Bank as shown in Fig.66.

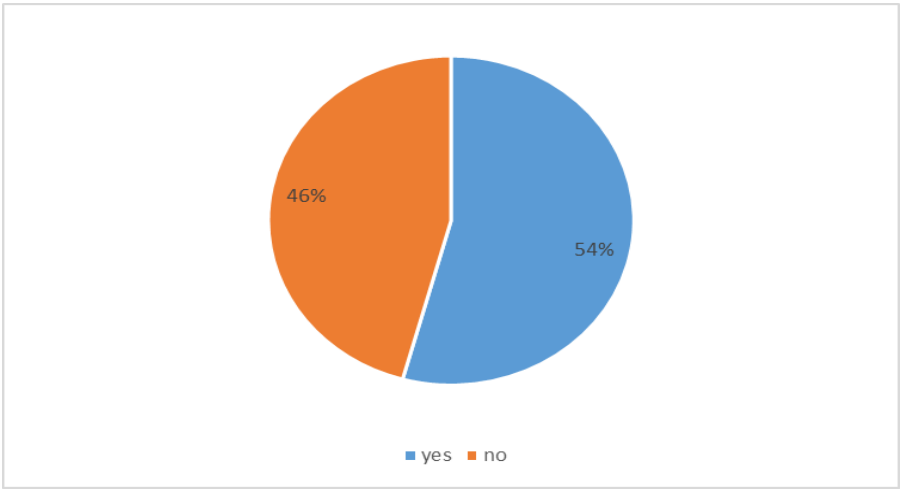


Fig. 65: Students with bank accounts

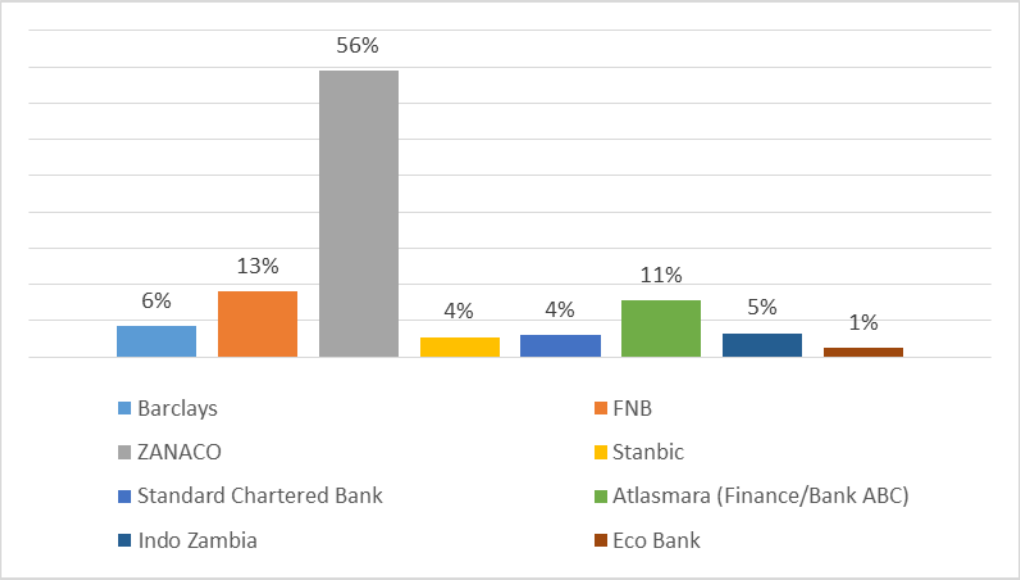


Fig. 66: Banks students have bank accounts with

4.2.6.2 Solutions recommended for the current payment system

Students were asked if a mobile bank transfer from a student account would resolve problems of long queues and omission of candidate payment details by institution of study. According to Fig.67, 65 percent of students said that a mobile bank transfer would resolve problems of long queues and omission of candidate payment details by institution of study while 7 percent disagreed. Further, 28 percent suggested other solutions such as developing an application that integrates the bank application with TEVETA, sending SMS reminders to students' mobile phones for payment deadlines and that TEVETA should consider two deadlines for payment of registration and examination fees.

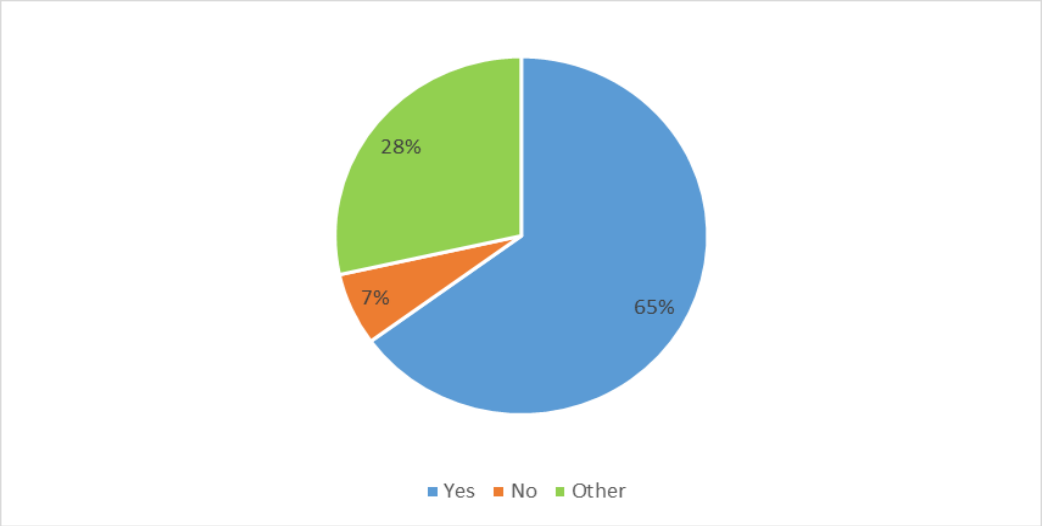


Fig. 67: Whether a mobile bank transfer would improve efficiency

4.3 System Implementation

The proposed system has two components; Web and USSD/SMS application. The web component was developed using PHP and HTML5. The web application runs on Apache web server and uses MYSQL database engine to store information. The web application allows users to use computers or smart phones with internet connection to send requests to the database in order to retrieve both examination enrolment details and examination results. The USSD/SMS mobile application was developed using Java programming language. The USSD/SMS mobile application requires a gateway which allows a mobile phone to send or receive requests to and from the mobile service provider. An individual or organisation needs to subscribe with mobile service provider in order to use a gateway. This proved expensive to the researcher and instead a USSD simulator was developed that allows students to access both examination enrolment details and examination results using a mobile phone.

4.3.1 WEB APPLICATION SUBSYSTEM FOR CANDIDATE REGISTRATION AND DISSEMINATION OF EXAMINATION RESULTS.

To enrol a candidate with TEVETA, a user needs to log in as a Data Entry Personnel using a web application. After enrolling a candidate, a student is automatically registered for examinations in courses (subjects) in that level and subsequent levels, thus eliminating some of the current business process where a student first fills in a student enrolment form and later on fill in an examination entry form in order to register for examinations. During examination results entry, authorised data entry personnel need to enter the student number to retrieve the details of a candidate such as student number, course code, level, year and a blank column for mark. During insertion of student marks, each mark is encrypted and hashed using AES encryption and SHA3-224 hash algorithms respectively. Encrypted marks and hashed marks of each student are stored in two independent databases for security reasons. Encrypted marks and hashed marks of student results are in table 15 and table 16 respectively. The snippet piece of code for secure insertion of marks using SHA3-224 hash algorithm and AES encryption algorithm are in table 12 and table 13 of section 3.4.1.

Table 15 Encrypted marks using AES encryption algorithm

Examnumber	Coursecode	Mark	Grade	Level	Year
5040	CS1	çUÇÂìmL‘ÿ^¶ƒÜ	P	I	2018
5040	CS2	[·À‰²óGhoÓMkñH	F	I	2018
5040	CS3	g×%üO—aT¸>f	D	I	2018
5040	CS4	g½!ghP–÷µ¦ŠQ	C	I	2018
5040	CS5	GmZOQ Q®#Ú°šÚ[–	M	I	2018
5040	CS6	jÎ€ÙJRIj€ÄO(óë	F	I	2018
5040	CS7	ƒ¥{!Èóç—Û)6;ÙA	P	I	2018

Table 16 Hashed marks using SHA3-224 hashing algorithm

Examnumber	Coursecode	Mark	Level	Year
5040	CS1	0095f800da7d48f4dfeb22808…	I	2018
5040	CS2	b595ca637d49a75bf266ea0af…	I	2018
5040	CS3	4bbad7a88024d334e4364e015…	I	2018
5040	CS4	8e050c050117bc630e87cb7c1…	I	2018
5040	CS5	0a57c09dc5f504de0d865714c…	I	2018
5040	CS6	629fbfe8a30cb576c956bf22d3…	I	2018
5040	CS7	b595ca637d49a75bf266ea0afa…	I	2018

Retrieval of Results

If the encrypted marks are not altered either during transmission or storage, an authorised student or stakeholder can use a web application to view results as shown in the screen in Fig.68. However, if encrypted student marks were altered during storage or transmission, the application detects through SHA3-224 algorithm and stop the grades from displaying as they are not authentic. Figure 69 shows the screen displayed when an attempt is made to retrieve results that were altered during transmission or storage. The snippet of code for secure retrieval of examination results using AES encryption algorithm and SHA3-224 hashing algorithm is in table 14 in section 3.4.2.

TEVETA

Statement of Results

STUDENT NUMBER	COURSE CODE	GRADE	LEVEL	YEAR
5040	CS1	P	1	2018
5040	CS2	P	1	2018
5040	CS3	C	1	2018
5040	CS4	F	1	2018
5040	CS5	F	1	2018
5040	CS6	F	1	2018
5040	CS7	F	1	2018

Fig. 68: Web screen showing results of a student

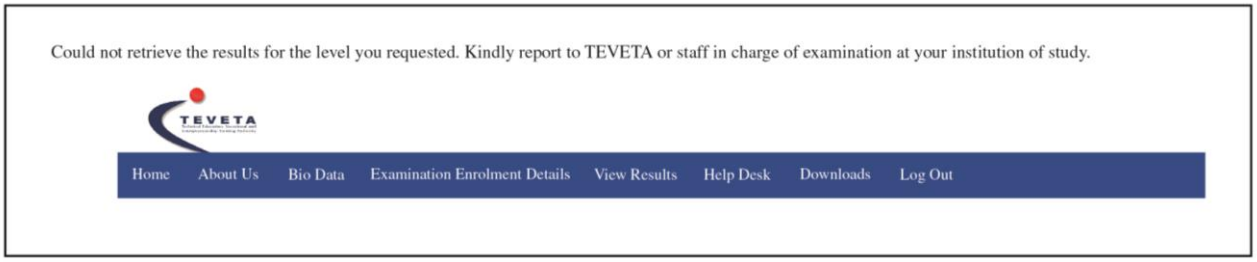


Fig. 69: Web Screen displayed when a user access altered examination results

4.3.2 MOBILE BASED APPLICATION SUBSYSTEM FOR DISSEMINATION OF EXAMINATION RESULTS

A student request for examination results by sending an SMS to a short code in a defined format. The format is examination number [space] Level [space] year of examination, then send the SMS to a number 400. For example, 5040 I 2018 and send to 400 as shown in Fig.70. Student gets feedback instantly through an SMS as shown in Fig.71. If marks were altered during transmission or storage, the application program detects through SHA3-224 algorithm and stops results from displaying shown in figure 72.

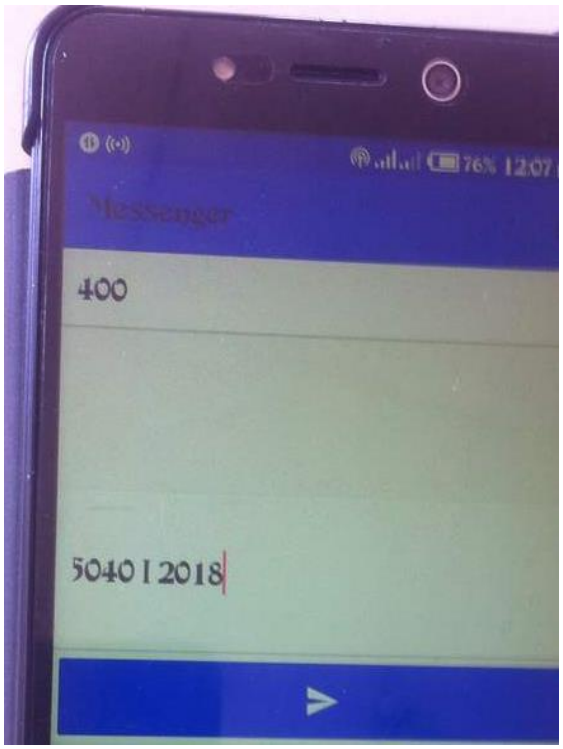


Fig.70: Mobile phone screen showing request for examination results

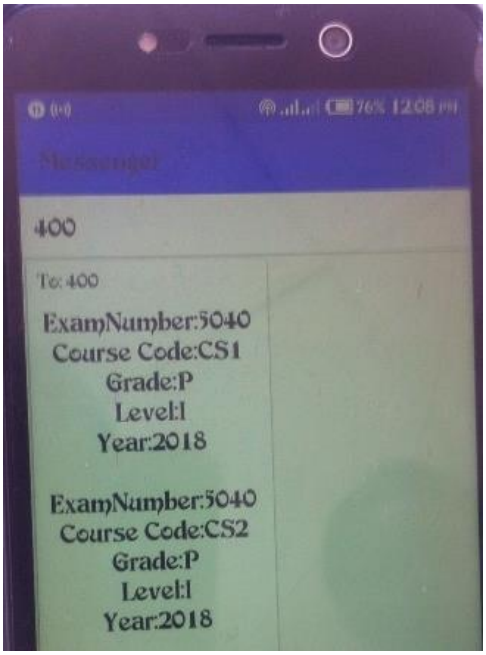


Fig.71: Mobile phone screen showing examination results

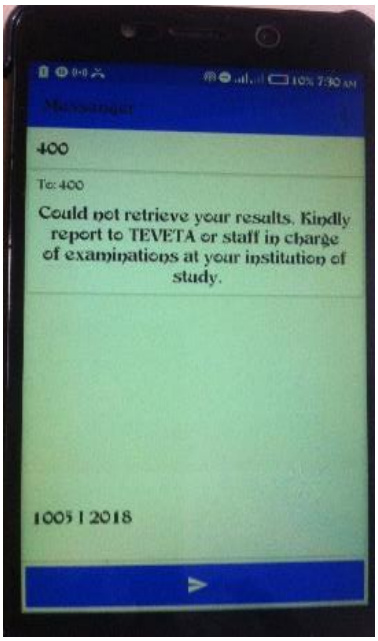


Fig. 72: Mobile phone screen displayed when user access altered examination results

Students can also request for course registration information by sending an SMS to a short code number in a defined format. The format is examination number [space] Level [space] year of examination. For example, 5040 I 2018 and send to 401 as shown in Fig.73. The student gets instant feedback of course registration data through an SMS. Figure 74 is a screen shot showing course registration details.

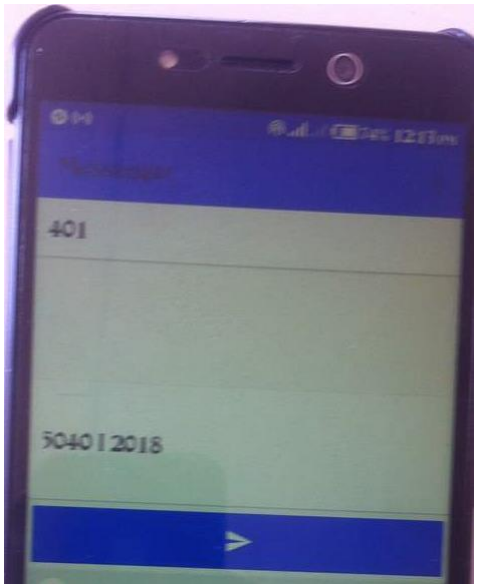


Fig.73: Mobile phone screen requesting course registration details

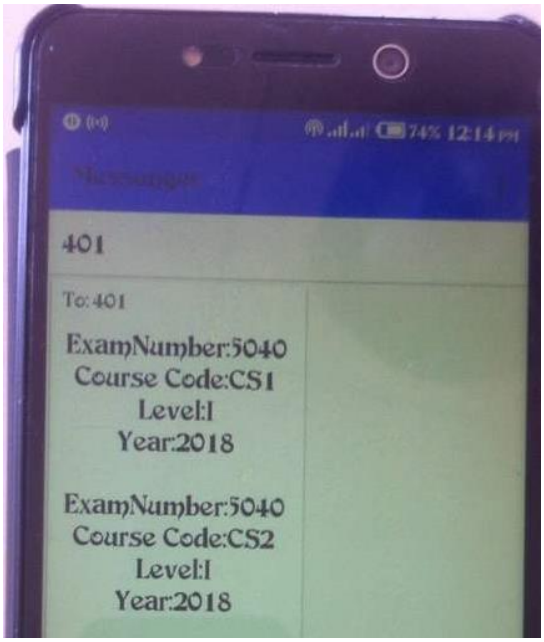


Fig.74: Mobile phone screen showing course registration details

4.4 Testing

The developed web based examination results dissemination system has been tested on different electronic platforms which include computers, tablets and smartphones with network connectivity with the local web server. The mobile application too has been tested on an android phone with network connectivity to the local web server. From the test results obtained, it can be concluded that a web and mobile based

examination results dissemination system using encryption and cryptographic hash functions not only provides secure means of storage and transmission of examination results but also an efficient means of disseminating results. Table 15 shows the system implementation testing evaluation of the prototype implementation.

Table 17 System implementation testing evaluation

Actor	TestID	Task	Scenario	Actual Results	Expected Results	Test Data	Comments
User	1	Login	The user authenticate herself/himself before accessing system functionality	The user was logged into the system upon providing the correct login credentials	The user was logged into the system upon supplying the correct login credentials and display a log in failure message	Username:0427 Password:123456	The login module worked as expected
User	2	Register candidate	The user entered details of a candidate to register for examinations	The student was successfully registered and a message was displayed on the screen.	When a student is successfully registered, he or she can view their course registration data through the web site or mobile phone.	Data such as exam number, institution name, programme, level, firstname, lastname, middlename, dateofbirth, nationality, national	Candidate was successfully registered.

						registration card number or passport were captured	
User	3	Update candidate details	The user enters the examination number for a candidate and application retrieves the candidate record to edit	The application retrieved a record for editing, made changes and the application successfully updated the information relating to a particular exam number by pressing on update button.	When the user enters the examination number for a candidate whose record needs editing, the application successfully, he or she should be able to edit the information relating to particular candidate. When the user press on update button, the record should be updated	Examination number: 5040	The record was successfully updated
user	4	Enter examination	The user enters the examination number for a candidate and application	The application retrieved candidate subject entries, entered marks and the application successfully encrypted marks using	When the user enters the examination number for the candidate to enter examination results, the application should retrieve	Examination number: 5040	Candidate results were successfully saved.

			retrieves the candidate subject entries	AES encryption algorithm and saved the results in the database. However, the user is unaware that marks are encrypted as everything happens while the application processes the information prior to transmission and storage of examination results.	the subject entries, he or she should be able to enter results relating to particular candidate. When the user press on save button, the application should encrypt marks using AES encryption algorithm.		
user	5	Verifying/ updating examination results	The user enters the examination number for a candidate and application retrieves the candidate results for verification or	The application retrieved candidate examination results, checked to verify that marks were correctly entered, if not, the user was able to edit marks and the application successfully updated	When the user enters the examination number for the candidate to verify/update examination results, the application should retrieve the examination, he or she should be able to edit results if they were incorrectly	Examination number: 5040	Candidate results were successfully verified and updated were necessary.

			update when the user discovers that marks do not tally with marks on mark sheets.	marks and encrypted them using AES encryption algorithm before saving in the database.	entered. When the user press on update button, the application should encrypt marks using AES encryption algorithm before storage in the database.		
User	6	Publishing results	The user enters the examination number for a candidate and application retrieves the candidate results to publish so that students/stakeholders can view them.	The application retrieved candidate examination results to publish so that students/stakeholders can view them. The user then clicked on the button publish and the application not only successfully encrypted the marks using AES encryption algorithm but also hashed each mark using SHA3-224 hashing	When the user enters the examination number for the candidate to publish examination results, the application should retrieve the examination, he or she should be able to publish examination results relating to particular candidate. When the user publish button, the application should not only encrypt marks using AES encryption algorithm but also	Examination Number: 5040	Candidate results were successfully published.

				algorithm to provide cyber security objectives of confidentiality, integrity and authenticity assurances on examination results	hash each mark using SHA3-224 hashing algorithm to provide cyber security objectives of confidentiality, integrity and authenticity assurances on examination results		
User	7	Viewing results	The user enters the examination number and level for a candidate and application retrieves the candidate results. If results were illegally modified, the application will detect and display an alert message	The application retrieved candidate examination results for the candidate. When results are illegally modified, application failed to decrypt the marks and display the examination results.	When the user enters the examination number and level for the candidate, the application should retrieve examination results if the results are not illegally modified. If results are illegally modified, the application should not display the results and instead display an alert message.	Examination Number: 5040	Candidate results were successfully viewed.

			that examination results could not be retrieved. If all is ok, the application will decrypt marks and proceed to display the results.				

4.5 Summary

In this chapter, the results of the baseline study and system implementation is presented. The baseline study revealed that TEVETA faced challenges in candidate registration for examinations. Further, factors that delay the release of examination results were also established. The participants recommended a mobile and web application for dissemination of examination results. The mobile and web applications for dissemination of examination results were developed using JAVA and PHP programming languages respectively. Both applications used AES encryption algorithm and SHA3-224 cryptographic hash function for secure storage and transmission of examination results. The results obtained from the text and evaluation of the developed prototype show that the system provides secure storage and transmission of examination results. This is largely because of encryption which provides confidentiality and hashing which provides integrity checks in case results are altered during storage or transmission.

CHAPTER FIVE
DISCUSSION AND CONCLUSION

5.1 Introduction

In this chapter, the discussion of research findings in Chapter 4 are presented. A discussion of business processes, system implementation, conclusion of the research and recommendations are presented.

5.2 Baseline study

The registration of candidates for examinations, processing of examination results and storage is done through a desktop application at TEVETA. The increase in the number of candidates sitting for examinations from a total of 10,493 in 2010 to 25, 650 in 2016 [20] has put a heavy strain on the examination body and has had challenges in the release of examination results on time. In order to improve efficiency in the release of the examination results, a baseline study was conducted to establish challenges faced by TEVETA in candidate registration for examinations and dissemination of examination results. The findings helped to come up with solutions that would improve efficiency in dissemination of examination results. Further, the baseline study also strived to establish availability of internet services and mobile phone network to TEVETA examined students in various parts of the country. This helped to establish whether the proposed system will be usable or not in various parts of the country.

5.2.1 Challenges with the TEVETA desktop application for candidate registration and examination results

The results of this research show that there were challenges with the desktop application used for candidate registration and processing of examination results. As indicated in Fig.46, challenges faced by TEVETA staff in candidate registration for examinations were as follows: 13 percent said incomplete registration forms, 13 percent said incorrect subject entries by candidates, 16 percent said registration forms received late, 9 percent said few personnel in data entry, 9 percent said large number of students, 3 percent said incorrect examination

numbers entered resulting into duplicate entries, 9 percent said TEVETA application failure to capture all students, 13 percent disparities in the number of students registered for examinations between the institution of study and TEVETA, 13 percent said failure by students to verify their details. As indicated in Fig.45, the challenges faced by members of staff in charge of examinations in TEVETA registered institutions were registration forms received late which accounted for 2 percent, 5 disparities in the number of students registered for examination between institutions of study and TEVETA accounted for 11 percent, 5 percent said incorrect examination numbers resulting into duplicate entries, 3 percent said incorrect subject entries, failure by students to verify their details accounted for 5 percent, incomplete registration forms accounted for 9 percent, non-submission of registration forms accounted for 5 percent, forms received late accounted for 9 percent, errors in data entry accounted for 13 percent, large number of students accounted for 6 percent, few personnel in data entry accounted for 11 percent, registration of illegal students accounted for 9 percent and other accounted for 2 percent, omission of candidate registration details sent to TEVETA accounted for 12 percent.

Figure 47 show that factors that delay the release of TEVETA students' examination results were long and tedious administrative procedures before the release of examination results which accounted for 33 percent, large number of students accounted for 25 percent, few personnel accounted for 34 percent, late submission of continuous assessment results by institutions accounted for 8 percent. An interview with a key IT staff also revealed irregularities in the way examination results are stored.

5.2.2 Suggested Solution

The respondents suggested solutions for mitigating challenges in candidate registration and dissemination of examination results. TEVETA IT staff that participated in the study suggested that a mobile and web application would improve dissemination of results. According to Fig.53, out of 514 students who participated in this study, 76 percent suggested that a mobile application can improve access to examination results, 21 percent were not sure while 3 percent disagreed. The study further show that 71 percent of students suggested that a web application can improve access to examination results, 26 percent were not sure while 3 percent disagreed according to Fig.56. This seem to suggest that the majority of the students are in favour of a mobile application than a web application although the difference in the percentages is 5 percent which is minimal.

5.2.3 Mobile Phone Network Providers

Having established that most students preferred a mobile application for dissemination of examination results, it was important to find out the mobile network provider available in their area and if students own their own mobile phone. According to Fig.55, the following were the mobile network provider available in areas where students reside (physical location away from the institution of study): Airtel only 22 percent, MTN only 4 percent, Zamtel only, Airtel and MTN 4 percent, Airtel and Zamtel 4 percent, MTN and Zamtel 1 percent, All Networks 61 percent. Furthermore the study revealed that 96 percent of students had mobile phones while 4 percent did not have as shown in Fig.54.

5.2.4 Internet accessibility

Figure 57 show that 82 percent of students use internet for academic or personal use while 18 percent do not use the internet. According to Fig.58, 57 percent of students accessed internet through mobile devices such as mobile phones and tablets, 17 percent accessed internet through their institution of study, 15 percent accessed the internet through mobile devices and institution of study, 5 percent accessed the internet through the internet café, 1 percent accessed the internet through public WI-FI only and other (combination of more than one method) accounted for 18 percent. This means that more students will be able to use the internet to access examination results through a web application.

5.3 Business Process Mapping and Modelling

This section discusses the business processes mapped and models designed in Chapter 3. It was established that although TEVETA uses a desktop application for candidate registration and processing of examination results, most of the processes were manual and used extensive paper. After reviewing the whole examination cycle from candidate registration to dissemination of examination results, a model was designed based on current TEVETA business processes and ISO 27001 information security standard for improved efficiency and secure storage and dissemination of examination results.

5.4 Implementation

This section discusses the implementation of the system presented in section 4.3 of Chapter 4. According to Fig.45 and Fig.46, challenges were faced with the current candidate registration system which indirectly impact the whole examination cycle and delay the release of examination results. Furthermore, specific factors that delay the release of examination results such as long administrative procedures were identified as indicated in Fig.47. The challenges can be reduced by automating the whole registration and examination results dissemination processes in order to scrap off most of intermediary processes.

The web based component implemented functionalities such as creating user accounts and updating user accounts, registering a candidate, updating candidate records, viewing candidate records, view course (subject) details, viewing results and generation of reports such as number of students who failed or passed in each course (subject). The mobile component implemented the functionality of viewing course (subject) details and viewing examination results. The requirements were derived from the current candidate registration and examination dissemination business processes. Interviews with key IT personnel and baseline study provided comprehensive information on challenges in candidate registration and examination results dissemination and storage.

Although many respondents recommended a web and mobile application for dissemination of examination results, it is important to improve the security in web and mobile based information applications because they are susceptible to cyber-attacks. Therefore, AES encryption algorithm and SHA3-224 cryptographic hash function were used in both a mobile and web application for dissemination of examination results to provide cyber security objectives of confidentiality, integrity and authenticity assurances on students' examination results. The web application was developed using PHP and the mobile application in Java. The developed prototype from the model shows that the system not only provides an efficient means of disseminating student examination results but also secure storage and transmission of examination results.

It can concluded that a web and mobile based examination results dissemination system is a feasible solution for efficient dissemination of examinations results while also providing secure storage and dissemination of examination results through encryption and cryptographic hash function.

5.5 Conclusion

TEVETA should strive to use modern technologies such as web and mobile applications in order to enhance the administration of national examinations more especially management of candidate registration and examination results information. In this study, a baseline study was conducted to establish the challenges faced by TEVETA and students regarding dissemination of examination results. Challenges have been identified and literature reviewed during the study show that similar challenges are also faced in other countries especially in Africa. Literature reviewed also show that cyber attacks on examination results system have occurred compromising the confidentiality, integrity and authenticity of students' examination results. The results from the baseline study and literature reviewed were used to develop a model based on TEVETA business processes for candidate registration, examination results entry, verification, publishing and dissemination of results. A web and mobile prototype utilizing encryption and cryptographic hash function was then developed based on model to provide information security objectives of confidentiality, integrity and encryption respectively. The developed prototype was tested and proved to be more secure because of encryption that provides confidentiality of examination results and hashing which provides a mechanism to detect altered students' examination results during transmission and storage.

5.6 Recommendations

As institutions of higher learning and examination bodies embrace web and mobile based examination results systems for efficient dissemination of examination results, it is important to improve the security in web and mobile based information applications because they are susceptible to cyber-attacks. Examination bodies and educational institutions should implement a web and mobile based students' examination results dissemination and verification system using encryption and cryptographic hash function for secure storage and dissemination of students' examination results. The weakest link in information security is the user. Therefore, higher learning instituitons and examination bodies must ensure that examination results are entered by Heads of Programmes/Departments or Programme Specialists only.

5.7 Future Works

The following are future research recommendations;

(a) Integrate the TEVETA application with Examinations Council of Zambia (ECZ) application for online verification of grades before a student is enrolled in a programme of study.

(b) Allow staff in charge of examinations in institutions of study to register candidates for examinations online and use of Closed-Circuit Television (CCTV) and Global positioning System (GPS) or Geographic Information System (GIS) in offices where candidate registration details are captured.

(c) Allow lecturers from various institutions of study to enter continuous assessment results online.

(d) Implement secure storage of the encryption/decryption key

(e) A fully-fledged mobile application to handle candidate registration and examination results entry.

5.8 Summary

The study brought out challenges faced in candidate registration and dissemination of examination results. The challenges are common in higher education institutions with many students. All the participants agreed that there were challenges in dissemination of examination results and that the challenges can be resolved through dissemination of results using a mobile and web application. A major contribution of this paper is in securing the storage and dissemination of examination results using AES encryption for confidentiality of examination results and SHA3-224 cryptographic hash function for detection of altered marks during storage and transmission of examination results.

REFERENCES

1 P. wallet, “Paper Commissioned for the Global education Monitoring Report 2016, Education for people and planet: Creating sustainable futures for all".,” 2016.

2 T. Frediksson, C. Barayre, P. Fajarnes, S. Fondeur, S. Lelmoli, D. Korka, S. Lakhe, M. P. Cuso and M. Pletosu, “The Information Economy Report 2017,” United Nations Publications, 2017.

3 N. S. Kumar and Z. Mihret, “Cyber Security in Developing World towards Excellency by 2026 - Opportunies, Policies,” *International Journal of Computer Sciences and Engineering,* vol. 5, no. 6, pp. 42-48, 2017.

4 K. Akarowhe, “Information Communication Technology (ICT) in the Educational System of the Third World Countries as a Pivotal to Meet Global Best Practice in Teachning and Development,” *American Journal of Computer Scuence and Information Technology,* vol. 5, no. 2, pp. 1-5, 2017.

5 K. Makanda, T. F. Vallent and H. Kim, “Remarks on National Cyber Security for Under Developed and Developed Countries: Focused on Malawi,” *American Journal of Engineering Research (AJER),* vol. 6, no. 7, pp. 257-260, 2017.

6 G. Emmanuel and A. S. Sife, “Challenges of managing information and communication technologies for education: experiences from Sokoine National Agriculture Library,” *International Journal of Education and Development using Information and Communication Technology,* vol. 4, no. 3, pp. 137-142, 2008.

7 P. Ziaie, “Challenges and issues of ICT industry in developing countries based on a case study of the barriers and the potential solutions for ICT development in Iran,” in *Computer Apllications Technology (CAT), 2013 International Conference*, 2013.

8 I. J. Ikenwe, O. M. Igbinovia and A. A. Elogie, “Information Security in the Digital Age: A Case of Developing Countries,” *Chinese Librianiship: an International Electronic Journal,* vol. 42, pp. 16-24, 2016.

9 M. S. Adrees, M. k. A. Omer and E. O. Sheta, “Cloud Computing Architecture for Higher Education in the Tird World Countries (Republic of Sudan as a Model),” *International Journal of Database Management Systems,* vol. 7, no. 3, pp. 13-24, 2015.

10 S. Okai, M. Uddin, A. Arshad, R. Alsaquor and A. Shah, “Cloud Computing Adoption Model fo Universities to increase ICT Proficiency,” 2014.

11 O. A. Ise, “A Novel Framework for Student Result Computation as a Cloud Computing Service,” American Journal of Systems and Software, vol. 3, no. 1, pp. 13-19, 2015.

12 E. R. Adagunodo, O. Awodele and S. Idowu, “SMS User Interface Result Checking System,” Issues in Informing Science and Technology, vol. 6, pp. 101-112, 2009.

13 M. I. Al Sheikh Eid, An Improved SMS User Interface System to Support University Services: A Case Study on Islamic University of Gaza, Islamic University of Gaza, 2011.

14 I. A. Muhamadi, A. A. Zaidan, M. A. Zaidan, C. Mapundu, B. B. Zaidan and R. S. Raja, "Auto Notification Service for the Student Record Retrieval System Using Short Message Service (SMS)," International Journal of Computer Science and Network Security, vol. 9, no. 8, pp. 200-208, 2009.

15 J. Zabangwa, Online and SMS Results Dissemination System (ORDS), University of Zambia, 2013.

16 M. Mshangi, E. N. Nfuka and C. Sanga, "Designing Secure web and Mobile-Based Information System For Dissemination of Students' Results: The Suitability Of Soft Design Science Methodology," International Journal of Computing and ICT Research, vol. 10, no. 2, pp. 10-40, 2016.

17 S. Rico, S. Sembhi and R. Singh-Latulipe, "Web Apllication Security: Sustainability Business and Risk Considerations," ISACA Journal, vol. 1, no. October, pp. 1-28, 2011.

18 D. Stufford and M. Pionto, The Web Application's Handbook: Finding and Exploiting Flaws, 2nd ed., Wiley Publishing, Inc, 2011.

19 N. E. Nfuka, C. Sanga and M. Mshangi, "The Rapid Growth of Cybercrimes Affecting Inofrmation Systems in the Global: Is this a Myth or Reality in Tanzania?," International Journal of Computer Science and Network Security, vol. 9, no. 8, pp. 200-208, 2014.

20 TEVET Newswriter, "A Publication of the Technical Education, Vocational and Entrepreneurship Training Authority," no. 2, April - June 2017.

21 TEVET Newswriter, "A Publication of the Technical Education, Vocational and Entrepreneurship Training Authority," no. 3, July- September 2017.

22 K.Martin, Everyday Cryptography: Fundamental Principles and Applications, New York: Oxford University Press, 2012.

23 E. Bala and C. D. Nyap, "A Software Application for Colleges of Education Student Results Proceesing," Journal of Information Engineering and Applications, vol. 2, no. 11, pp. 12-24, 2012.

24 A. A. Eludire and I. Arakeji, "The Design and Implementation of Student Academic Management System," Research Journal of Applied Sciences, Engineering and Technology, vol. 3, no. 8, pp. 707-712, 2011.

25 E. O. Ukem and F. A. Ofoegbu, "A Software Application for University Students Results Processing," Journal of Theoretical and Apllied Information technology, vol. 35, no. 1, pp. 34-43, 2012.

26 B. Milumbe, J. Phiri and M. M. Kalumbilo, "Automation of the Candidate

Registration For School Examinations in Zambia Using the Cloud Model," in IEEE International Conference in Information and Communications Technologies (ICICT), Lusaka, 2017.

27 L. Solomom and J. Phiri, "Enhancing the Administration of National Examinations Using Mobile Cloud Technologies: A case of Malawi National Examinations Board," IJACSA (International Journal of Computer Science and Computer Applications), vol. 9, no. 8, 2017.

28 A. U. Osagie and A. Mallam, "Data Analysis and Result Computation (DARC) Algorithm for tertiary Institutions," Journal of Computer Engineering, vol. 14, no. 3, pp. 63-69, 2013.

29 Verizon, "2017 Data Breach Invesitigation Report," 2017.

30 N. Perlroth, "Hackers Breach 53 Universities and Dump Thousands of Personal Records Online," 2012. [Online]. Available: https://bits.blogs.nytimes.com/2012/10/03/hackers-breach-53-universities-dump-thousands-of-personal-records-online/. [Accessed 25 July 2018].

31 BBC, "Greenwich University fined £120,000 for data breach," 21 May 2018. [Online]. Available: https://www.bbc.com/news/technology-44197118. [Accessed 25 July 2018].

32 B. W. Okibo and O. B. Ochibe, "Challenges Facing Inofrmation Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa - Kenya," International Journal of Management Excellence, vol. 3, no. 1, pp. 336-349, 2014.

33 Capital Campus, "KU, JKUAT top list of students hacking systems to change grades, fees," 2015. [Online]. Available: https://www.capitalfm.co.ke/campus/ku-jkuat-top-list-of-students-hacking-systems-to-change-grade-fees/. [Accessed 25 July 2018].

34 A. Ndolo, S. Ogara and S. Liyala, "Model for Information Security Government Prediction in Public Universities in Kenya," International Journal of Computer Applications Technology and Research, vol. 7, no. 2, pp. 63-77, 2018.

35 P. Juma, "Hackers blamed in KU exam row," 1 December 2011. [Online]. Available: https://www.nation.co.ke/news/Hackers-blamed-in-KU-exam-row--/1056-1282692-3u0d8mz/index.html. [Accessed 3 August 2018].

36 R. Mugyenyi, "Analysing Information Systems Security In Higher Learning Institutions of Uganda," International Journal of Scientific & Technology Research, vol. 6, no. 10, 2017.

37 R. Marchany, "Higher Education: Open and Secure," SANS Analyst Survey, 2014.

38 K. U. Singh, J. Chanchala and N. Gaud, "Measurement of Security Dangers in University Network," International Journal of Computer Applications, vol. 155, no. 1, pp. 5-10, 2016.

39 Certified Information Systems Security Professional, Wiley Publishing, 2008.

40 T. D. Fishman, C. Clark and J. L. Grama, “Elevating cybersecurity on the higher education leadership agenda,” Deloitte Insights, 2018.

41 M. Magomelo, P. Mamboko and T. Tsokota, “The Status of Information Security Governance within State Universities in Zimbabwe,” Journal of Emerging Trends in Computing and Information Sciences, vol. 5, no. 8, pp. 710-727, 2014.

42 S. K. Cheung, “Information Security Management for Higher Education Institutions,” in Preceeding of the First Euro-China Connference On Intelligent Data Analysis and its Applications, Shenzhen, China, 2014.

43 B. G. Raggard, Information Security Management: Concepts and Principles, CRC Press, 2010.

44 J. R. Vacca, Computer and Information Security Handbook, Morgan Kaufmann Publishers, 2009.

45 M. Rhodes-Ousley, Information Security: The Complete Reference, McGraw-Hill Companies, 2013.

46 N. Singhal and S. Singhal, “A Comparative Analysis of AES and RSA Algorithm,” International Journal of Scientific & Engineering Research, vol. 7, no. 5, pp. 149-151, 2016.

47 P. Luo, Y. Fei, L. Zhang and A. A. Ding, “Differential Fault Analysis of SHA3-224 and SHA3-256,” 2016.

48 A. A. Nasser, “Information security gap analysis based on ISO 27001:2013 Standard: A ase Study of the Yemeni Academy for,” International Journal of Scientific Research in Multidisciplinary Studies Graduate Studies, Sana'a, Yemen, vol. 3, no. 11, pp. 4-13, 2017.

49 H. Chan and S. Mubarak, “Significance of Information Security Awareness in the Higher Education Sector,” International Journal of Computer Applications, vol. 60, no. 10, pp. 23-31, 2012.

50 A. Marks and Y. Rezgui, “Information Security Awareness in Higher Education: An Exploratory Study,” Computers and Security, vol. 27, no. 7, pp. 241-253, 2008.

51 S. Hina and D. D. Dominic, “Information Security Policies' Compliance: A Perspective for Higher Education Institutions,” Journal of Computer Information Systems, 2018.

52 L. Muniandy, B. Muniandy and Z. Samsudin, “Cyber Security Behaviour among Higher Education Students in Malaysia,” Journal of Information Assurance & Cyber Security, pp. 1-13, 2017.

53 M. S. Eyadat, “Higher Education Administrators Roles in Fortification of Information Security Program,” Journal of Academic Administration in Higher Education, vol. 11, no. 2, pp. 61-68, 2015.

54 A. I. Al-Alawi, S. M. Al-Kandari and R. H. Abdel-Razek, “Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University,” Journal of Innovation and Business Best Practice, pp. 1-23, 2016.

55 H. D. Bruijn and M. Janssen, “Building Cyber Security Awareness: The need for evidence-based framing strategies,”Government Information Quartely, vol. 34, pp. 1-7, 2017

56 M. Magomelo, P. Mamboko and T. Tsokota, “The Status of Information Security Governance within State Universities in Zimbabwe,” Journal of Emerging Trends in Computing and Information Sciences, vol. 5, no. 8, pp. 710-727, 2014.

57 R. Chandarman and V. Niekerk, “Student's cybersecurity Awareness at a Private Tertiary Educational Institution,” The African Journal of Information and Communication (AJIC), vol. 20, pp. 133-155, 2017.

58 E. Antwi-Bekoe and S. G. Nimako, “Computer Security Awareness and Vulnerabilities: An Explanatory Study for Two Public Higher Institutions in Ghana,” Journal of Science and Technology, vol. 1, no. 7, 2012.

59 K. K. Adu and E. Adjei, “The phenomenon of data loss and cyber security issues in Ghana,” Emerald Publishing Limited, 2018.

60 W. Stallings, Cryptography and Network Security: Principles and Practices, 4th ed., Upper Saddle River, NJ 07458: Pearson Education, Inc., 2006.

61 J. R. Ndiege and O. G. Okello, “Information Security Awareness Amongst Students Joining Higher Academic Institutions in Developing Countries: Evidence from Kenya,” The African Journal of Information Systems, vol. 10, no. 3, pp. 204-221, 2018.

62 Minister of Transport and Communication, Mr Mushimba, Ministerial Statement on the Information and Communication Technologies and Electronic Government, 2017.

63 Ministry of Communications and Transport, National Information and communication Technology Policy, 2006

64 L. Simusokwe, “Cyber Crime and the Law in Zambia,” 2009.

65 ISO/IEC 2005, Information technology - Security techniques - Information security management systems - Requirements, 2005.

66 G. Disterer, “ISO/IEC 27000, 27001 and 27002 for Information Security Management,” Journal of Information Security, vol. 4, pp. 92-100, 2013.

67 T. Mataracioglu and S. Ozkan, “Governing Information Security in Conjuction with COBIT and ISO 27001,” International Journal of Network Security & its Applications, vol. 3, no. 4, pp. 11-116, 2011.

68 Z. Ismail, M. Masrom, Z. M. Sidek and D. S. Hamzah, “Framework to Manage Information Security for Malaysian Academic Environment,” Journal of Inofmration

Assurance & CyberSecurity, pp. 1-16, 2010.

69 M. A. Talib, M. E. Barachi, A. Khelifi and O. Ormandjieve, “Guide to ISO 27001: UAE Case Study,” in Issues in Information Science and Information Technology, 2012.

70 A. A. Nasser, “Information security gap analysis based on ISO 27001:2013 Standard: A ase Study of the Yemeni Academy for,” International Journal of Scientific Research in Multidisciplinary Studies Graduate Studies, Sana'a, Yemen, vol. 3, no. 11, pp. 4-13, 2017.

71 ISO 27001, “Information Technology, Security Techniques, Information Security Management Systems, Requirements,” Geneva, 2005.

72 Z. Hercigonja, D. Gimnazija and V. Croatia, “Comparative Analysis of Cryptographic Algorithms,” International Journal of Digital technology & Economy, vol. 1, no. 2, pp. 127-134, 2016.

73 W. Stallings, Cryptography and Network Security: Principles and Practice, 6th ed., PHI, 2014.

74 B. Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C, 2nd ed., John Wiley & Sons, 1995.

75 D. Khovratovich, C. Rechberger and A. Savelieva, 2011. [Online]. Available: https://eprint.iacr.org/2011/286.pdf. [Accessed 27 July 2018].

76 M. J. Dworkin, “SHA-3 Standard: Permutation-Based Hash and Extendable- Output Functions,” 4 August 2015. [Online]. Available: https://www.nist.gov/publications/sha-3-standard-permutation-based-hash-and-extendable-output-functions?pub_id=919061. [Accessed 27 July 2018].

77 National Institute of Standards and Technology, “SHA-3 Standard:,” Federal Information Processing Standards Publication, 2015.

78 Boxcryptor, “AES and RSA Encryption,” [Online]. Available: https://www.boxcryptor.com/en/encryption. [Accessed 13 July 2018].

79 P. Mahajan and A. Sachdeva, “A Study of Enryption Algorithms aES, DES and RSA for Security,” Global Journal of Computer Science and Technology Network, Web & Security, vol. 13, no. 15, 2013.

80 M. A. Mushtaque, “Comparison Analysis on Different parameters of Encryption Algorithms for Information Security,” International Journal of Computer Sciences & Engineering, vol. 2, no. 4, pp. 76-82, 2014.

81 O. A. Afolabi and O. G. Atanda, “Comparative Analysis of Some Selected Cryptographic Algorithms,” Computing, Information Systems, Development Informatics & Allied Research Journal, vol. 7, no. 2, pp. 41-52, 2016.

82 K. Graves, Certified Ethical Hacker Study Guide, Wiley Publishing, Inc, 2010.

83 D. Kaur and P. Kaur, “Empirical Analysis of Web Attacks,” in International Conference on Information Security & Privacy (ICISO2015), Nagpur, INDIA, 11-12 December 2015.

84 T. Mirzoev, M. Brannon, S. Lasker and M. Miller, “Mobile Application Threats and Security,” World of Computer Science and Information Technology Journal (WCSIT), vol. 4, no. 5, pp. 57-61, 2014.

85 N. Mckelvey, “Data Protection Issues in Higher Education with technological Advancements,” International Journal of Evaluation and Research in Education, vol. 3, no. 3, pp. 133-141, 2014.

86 S. A. Idowu and A. O. Osofisan, “Cloud Computing and Sustainable Development in Higher education,” Journal of Emerging Trends in Computing and Information Sciences, vol. 3, no. 11, pp. 1466-1471, 2012.

87 S. Matthew, “Implementation of the Cloud Model in Education - A Revolution,” International Journal of Computer Theory and Engineering, vol. 4, no. 3, p. 473475, 2012.

88 S. Palaniappan, “Cloud Computing for Academic Environment,” International Journal of Computer Science and Mobile Computing, vol. 3, no. 5, pp. 8-15, 2014.

89 S. Satpute and S. B. Deora, “International Journal of advanced Research in Computer Science,” Cloud-Based Storage for Education, vol. 4, no. 3, pp. 77-80, 2013.

90 F. Karim and R. Giselle, “Cloud Computing in Education in Developing Countries,” Computer and Information Science, vol. 10, no. 2, pp. 87-96, 2017.

91 F. Makoza, “Cloud Computing adoption in Higher Education Institutions of Malawi: An exploratory study,” Journal of Computing and ICT Research, vol. 9, no. 2, pp. 37-54, 2016.

92 K. H. A. Al-Shqeerai, M. R. Hassan, F. M. A. Al-Shrouf and H. Fajraoui, “Cloud Computing Security Challenges in Higher Education Institutions,” International Journal of Computer Applications, vol. 161, no. 6, pp. 23-29, 2017.

93 O. O. Olusanya and O. Ogaba, “Result Alert System through SMS and Email,” IOSR Journal of Moble Computing & Computing, vol. 2, no. 2, pp. 41-45, 2015.

94 A. A. Obiniyi and A. E.-S. Ezugwu, “Design and Implementation of Students' Information system for Tertiary Institutions Using Neural Networks: An Open Source Approach,” International Journal Of Green Computing, vol. 1, no. 1, pp. 1-15, 2010.

95 F. Rantiola, E. Ozichi, A. Abiodun, G. Ishaya and O. Damilola, “Development of a Multifactor Authentication Result Checking System through GSM,” Computer Applications: An International Journal (CAIJ), vol. 1, no. 2, pp. 1-8, 2014.

96 J. Mukarukundo, “Design and Implementation of Mobile Application for Results Dissemination System,” Journal of Software Engineering and Applications, vol. 10, pp. 787-791, 2017.

97 P. Joshi, P. Panday and N. Kuchankar, “Implementation Paper of Results Alert System,” International Journal for research in Applied Science & Engineering Technology (IJRASET), vol. 5, no. 3, pp. 561-563, 2017.

98 L. Mseteka and J. Phiri, “A Secure Model for Storage and Dissemination of Examination Results: A Case of Zambia Technical Education Vocational and Entrepreneurship Training Authority (TEVETA)”, Journal of Computer Science, 2019.

99 L. Mseteka, J. Phiri, S. Tembo “Web and Mobile Based Examination Results Dissemination and Verification system using Authenticated Encryption: A case of Zambia Technical Education Vocational and Entrepreneurship Training Authority (TEVETA)”, International Journal of Future Computer and Communications (IJFCC), 2019.

100 X. Jia, Object-Oriented Software Development using Java, 2nd Edition ed., Pearson Education, Inc, 2003.

101 C. R. Kothari, Research Methodology: Methods & Techniques, New Age International (P) Ltd, 2004.

102 J. Jonker and B. Pennink, The Essence of Research Methodology: A Concise Guide for Master and phD Students in Management Science, Springer, 2010.

103 A. Moazzarn, "Sampling & Sample Size Estimation," 2014.

APPENDICES

Appendix 1: Code Listing

WEB APPLICATION FOR DISSEMINATION OF EXAMINATION RESULTS

Enrol.php (Script that processes candidate registration details)

```
<?
include 'config.php';
include 'config2.php';
if (isset($_POST['studentid'])){
// remove backslashes
$yearenrol= stripslashes($_REQUEST['yearenrol']);
$yearenrol = mysqli_real_escape_string($link,$yearenrol );
$studentid= stripslashes($_REQUEST['studentid']);
//escapes special characters in a string
$studentid= mysqli_real_escape_string($link,$studentid);
$spassword= stripslashes($_REQUEST['spassword']);
$spassword= mysqli_real_escape_string($link,$spassword);
$institution= stripslashes($_REQUEST['institution']);
$institution= mysqli_real_escape_string($link,$institution);
$programme= stripslashes($_REQUEST['programme']);
$programme= mysqli_real_escape_string($link,$programme);
$level= stripslashes($_REQUEST['level']);
$level= mysqli_real_escape_string($link,$level);
$fname= stripslashes($_REQUEST['fname']);
$fname= mysqli_real_escape_string($link,$fname);
$mname= stripslashes($_REQUEST['mname']);
$mname= mysqli_real_escape_string($link,$mname);
$lname = stripslashes($_REQUEST['lname']);
$lname= mysqli_real_escape_string($link,$lname);
$gender= stripslashes($_REQUEST['gender']);
$gender= mysqli_real_escape_string($link,$gender);
$birth = stripslashes($_REQUEST['birth']);
$birth = mysqli_real_escape_string($link,$birth);
$nationality= stripslashes($_REQUEST['nationality']);
$nationality= mysqli_real_escape_string($link,$nationality);
$nrc= stripslashes($_REQUEST['nrc']);
$nrc= mysqli_real_escape_string($link,$nrc);
$passport= stripslashes($_REQUEST['passport']);
$passport= mysqli_real_escape_string($link,$passport);

//$stored_password = md5(trim($password));

//
$query = "SELECT * FROM studentdetails WHERE studentnumber='$studentid'";
        $check = mysqli_query($link,$query) or die(mysql_error());
```

```
        $rows = mysqli_num_rows($check);
      if($rows==1){

            echo "This student has already been enrolled.  <a href='inserttest.php'>Back to Registration Form</a></div>";
                  echo "<br>";

       }else{
/* Insert record */
$newquery ="INSERT INTO studentdetails SET studentnumber='{$studentid}',password='".md5($spassword)."',institution='{$institution}',programmename='{$programme}',Level= '{$level}', year_of_enrolment ='{$yearenrol}', firstname='{$fname}',lastname='{$lname}',othername='{$mname}',gender='{$gender}',dateofbirth ='{$birth}',nrcno= '{$nrc}',nationality='{$nationality}',passport='{$passport}'";
if (mysqli_query($link, $newquery))
{ echo "";
} else {
        echo "Error:".$newquery. "<br>".mysqli_close($link);
}
}
}
echo "Click on Save to complete the registration and examination enrolment process";
?>
  <form id="form2" name="form2" method="POST" action="exam_enrol.php">
  <fieldset><legend>Examination Enrolment Details </legend>
 <table width="840" border="0">
  <tr>
      <td><input type="submit" name="saveBtn" id="saveBtn" value="Save" /></td>
    </tr>
  <tr>
<td width="245">Student Number</td>
<td width="143">Course Code</td>
<td width="87">Year Enrolled</td>
<td width="87">Level</td>
</tr>
<?
$retrieve2=mysqli_query($link, "SELECT * FROM Studentdetails as s, course as c where s.programmename=c.programmename AND c.programmename='$programme' AND C.Level = '$level' and s.studentnumber ='$studentid'");

while($nrow = mysqli_fetch_array($retrieve2))
  {
 echo"<td><input type='text' name='studentNumber[]' value='".$nrow['studentnumber']."' readonly></td>";
 echo"<td><input type='text' name='subjectcode[]' value='".$nrow['coursecode']."' readonly></td>";
 echo"<td><input type='text' name='Year[]' value='".$nrow['year_of_enrolment']."' readonly></td>";
 echo"<td><input type='text' name='Level[]' value='".$nrow["Level"]."' readonly></td>";
 echo "</tr>";
```

```
  }
?>
```

Examenrol.php (script that processes candidate enrolment details)

```
<?
include 'config.php';
if(isset($_POST["saveBtn"])){
$studentNumber = $_POST['studentNumber'];
$subjectcode = $_POST['subjectcode'];
$Year = $_POST['Year'];
$Level = $_POST['Level'];
if ($studentNumber== '0' && $subjectCode == '0' && $Year == '0' && $Level == '0' ) {
echo "0";
} else {

$queries = array();
for ($i = 0; $i < count($studentNumber); $i++) {
if (!get_magic_quotes_gpc()) {
$subjectcode[$i] = addslashes($subjectcode[$i]);
$studentNumber[$i] = addslashes($studentNumber[$i]);
$Year[$i] = addslashes($Year[$i]);
$Level[$i] = addslashes($Level[$i]);

}
$queries[] = "('$studentNumber[$i]','$subjectcode[$i]','$Level[$i]','$Year[$i]')";

}

if (count($queries) == 0) {
# Nothing passed
# exit
}
$values = implode(", ", $queries);
$insert ="INSERT INTO test(studentnumber, coursecode, level, year)VALUES $values";
$result = mysqli_query($link,$insert) or die(mysqli_error($link));
echo "Record successfully registered";
echo "
<br/> <a href='enn2.php'>Enrol new Student</a></div>";

  }
}

  ?>
```

Results Entry scripts

Coursedetails.php (retrieve examination enrolment details and allows Data entry personnel to enter results)

```
<?
include 'config.php';
extract ($_POST);
if (!$link) {
die("Connection failed: " . mysqli_connect_error());
}
/* retrieve record */
$result = mysqli_query($link, "SELECT SerialNumber, studentnumber, coursecode, mark, level, year FROM results where studentnumber='$studentid'");
while($row = mysqli_fetch_array($result))
  {
$serialnumber = $row['SerialNumber'];
$studentid = $row['studentnumber'];
 $coursecode = $row['coursecode'];
  $mark = $row[mark’];
   $level = $row['level'];
   $year = $row['year'];
   echo"<td><input type='text' name='serialnumber[]' value='".$row['SerialNumber']."' readonly></td>";
  echo"<td><input type='text' name='studentid[]' value='".$row['studentnumber']."' readonly></td>";
 echo"<td><input type='text' name='coursecode[]' value='".$row['coursecode']."' readonly </td>";
  echo"<td><input type='text' name='mark[]' value='".$row['mark’]."' </td>";
 echo"<td><input type='text' name='level[]' value='".$row['level']."' readonly></td>";
 echo"<td><input type='text' name='year[]' value='".$row["year"]."' readonly></td>";
 echo "</tr>";
  }
?>
 <tr>
      <td><input type="submit" name="saveBtn" id="saveBtn" value="Submit Results" /></td>
       <td><input type="reset" name="cancel" id="cancel" value="Cancel" /></td>
     </tr>
     </table>
</div>
</body>
</html>
```

ENTER RESULTS

Resultsentry.php (script that processes script processes results entered by Data Entry personnel)

```
<?

include 'config.php';
include 'config2.php';
include 'pk.php';
if(isset($_POST["saveBtn"])){
$studentid =$_POST['studentid'];
$serialnumber =($_POST['serialnumber']);
$countserialnumber =count($_POST['serialnumber']);
$coursecode =$_POST['coursecode'];
$mark =$_POST['mark'];
$level =$_POST['level'];
$year =$_POST['year'];
for ($i=0;$i<$countserialnumber;$i++) {
if (!get_magic_quotes_gpc()) {
$coursecode[$i] = addslashes($coursecode[$i]);
$studentid[$i] = addslashes($studentid[$i]);
$serialnumber[$i] = addslashes($serialnumber[$i]);
$mark[$i] = addslashes($mark[$i]);
$year[$i] = addslashes($year[$i]);
$level[$i] = addslashes($level[$i]);
$mark[$i] = addslashes($mark[$i]);
$hashmark[$i]=hash('sha256',$mark[$i]);
$queries = array();
$queries[] = "('$serialnumber[$i]','$studentid[$i]','$coursecode[$i]','$hashmark[$i]','$level[$i]','$year[$i]')";
if (count($queries) == 0) {
# Nothing passed
# exit
}
$values = implode(", ", $queries);
//
$query1 ="SELECT * FROM hashedmarks WHERE serialnumber='$serialnumber[$i]'";
$check = mysqli_query($link2,$query1);
//echo $query1;
$rows = mysqli_num_rows($check);
if($rows>0){
echo "Results for this student have already been entered. Please contact the staff in-charge of updating results to update the results. <a href='enter_results.php'>Back</a></div>";
                    echo "<br>";
                    die (mysqli_error($link2));
                    mysqli_close($link2);
                     }else{
$insert="INSERT INTO hashedmarks(serialnumber, studentnumber, coursecode,mark, level, year)VALUES $values";
```

```
$result = mysqli_query($link2,$insert) or die(mysqli_error($link2));
//
$update=mysqli_query($link, "UPDATE results SET studentnumber='$studentid[$i]',coursecode='$coursecode[$i]',mark=AES_ENCRYPT('$mark[$i]','$key'), level='$level[$i]',year='$year[$i]' where SerialNumber='$serialnumber[$i]'");
  }
  }
  }
}
if($update)
{
echo "Student results successfully saved";
echo "<br>";
echo "
<br/> <a href='enrolment.php'>Back</a></div>";
}
mysqli_close($link);
?>
```

UPDATE RESULTS
retrieveresultstoupdate.php (retrieve results to update)

```
include 'config.php';
include 'pk.php';
extract ($_POST);
if (!$link) {
die("Connection failed: " . mysqli_connect_error());
}
/* retrieve record */
$result = mysqli_query($link, "SELECT SerialNumber, studentnumber, coursecode, AES_DECRYPT(mark,'$key'), grade, level, year FROM results where studentnumber='$studentid'");
while($row = mysqli_fetch_array($result))
  {
$serialnumber = $row['SerialNumber'];
$studentid = $row['studentnumber'];
 $coursecode = $row['coursecode'];
  $mark = $row["AES_DECRYPT(mark,'$key')"];
   $level = $row['level'];
   $year = $row['year'];
 echo"<td><input type='text' name='serialnumber[]' value='".$row['SerialNumber']."' readonly></td>";
  echo"<td><input type='text' name='studentid[]' value='".$row['studentnumber']."' readonly></td>";
 echo"<td><input type='text' name='coursecode[]' value='".$row['coursecode']."' readonly </td>";
  echo"<td><input type='text' name='mark[]' value='".$row["AES_DECRYPT(mark,'$key')"]."' </td>";
 echo"<td><input type='text' name='level[]' value='".$row['level']."' readonly></td>";
 echo"<td><input type='text' name='year[]' value='".$row["year"]."' readonly></td>";
```

```
 echo "</tr>";
  }

?>
```

Updatestudentsresults.php (script that updates students results)

```
<?
include 'config.php';
include 'config2.php';
include 'pk.php';
if(isset($_POST["saveBtn"])){
$studentid =$_POST['studentid'];
$serialnumber =($_POST['serialnumber']);
$countserialnumber =count($_POST['serialnumber']);
$coursecode =$_POST['coursecode'];
$mark =$_POST['mark'];
$level =$_POST['level'];
$year =$_POST['year'];
for ($i=0;$i<$countserialnumber;$i++) {
if (!get_magic_quotes_gpc()) {
$coursecode[$i] = addslashes($coursecode[$i]);
$studentid[$i] = addslashes($studentid[$i]);
$serialnumber[$i] = addslashes($serialnumber[$i]);
$mark[$i] = addslashes($mark[$i]);
$year[$i] = addslashes($year[$i]);
$level[$i] = addslashes($level[$i]);
$mark[$i] = addslashes($mark[$i]);
$update=mysqli_query($link, "UPDATE results SET
studentnumber='$studentid[$i]',coursecode='$coursecode[$i]',mark=AES_ENCRYPT('$mark
[$i]','$key'),level='$level[$i]',year='$year[$i]' where SerialNumber='$serialnumber[$i]'");
}
}
}
if(isset($_POST["saveBtn"])){
$studentid =$_POST['studentid'];
$serialnumber =($_POST['serialnumber']);
$countserialnumber =count($_POST['serialnumber']);
$coursecode =$_POST['coursecode'];
$mark =$_POST['mark'];
$level =$_POST['level'];
$year =$_POST['year'];
if ($studentid== '0' && $serialnumber== '0'&& $coursecode == '0' && $mark == '0' &&
$year == '0' && $level == '0' ) {
echo "0";
} else {
$queries = array();
for ($i = 0; $i<$countserialnumber; $i++) {
if (!get_magic_quotes_gpc()) {
$coursecode[$i] = addslashes($coursecode[$i]);
```

```
$studentid[$i] = addslashes($studentid[$i]);
$serialnumber[$i] = addslashes($serialnumber[$i]);
$mark[$i] = addslashes($mark[$i]);
$hashmark[$i]=hash('sha3-224',$mark[$i]);
$year[$i] = addslashes($year[$i]);
$level[$i] = addslashes($level[$i]);
}
$queries[] =
"('$serialnumber[$i]','$studentid[$i]','$coursecode[$i]','$hashmark[$i]','$level[$i]','$year[$i]')"
;
$values = implode(", ", $queries);
$insert ="UPDATE hashedmarks SET
studentnumber='$studentid[$i]',coursecode='$coursecode[$i]',mark='$hashmark[$i]',level='$l
evel[$i]',year='$year[$i]' where SerialNumber='$serialnumber[$i]'";
$result = mysqli_query($link2,$insert) or die(mysqli_error($link2));
  }
  }
  }
if($update)
{
echo "Student results successfully updated";
echo "<br>";
echo "
<br/> <a href='updateresults.php'>Back</a></div>";
}
mysqli_close($link);
?>
```

PUBLISH RESULTS

Publishfinalresults.php (script publishes final results and allows students to view their grades)

```
<?
include 'config.php';
include 'config2.php';
include 'pk.php';
if(isset($_POST["saveBtn"])){
$studentid =$_POST['studentid'];
$serialnumber =($_POST['serialnumber']);
$countserialnumber =count($_POST['serialnumber']);
$coursecode =$_POST['coursecode'];
$mark =$_POST['mark'];
$grade=$_POST['grade'];
$level =$_POST['level'];
$year =$_POST['year'];
for ($i=0;$i<$countserialnumber;$i++) {
if (!get_magic_quotes_gpc()) {
$coursecode[$i] = addslashes($coursecode[$i]);
$studentid[$i] = addslashes($studentid[$i]);
$serialnumber[$i] = addslashes($serialnumber[$i]);
```

```
$mark[$i] = addslashes($mark[$i]);
$year[$i] = addslashes($year[$i]);
$level[$i] = addslashes($level[$i]);
$mark[$i] = addslashes($mark[$i]);
$grade[$i] = addslashes($grade[$i]);
$update=mysqli_query($link,"UPDATE TEST SET
studentnumber='$studentid[$i]',coursecode='$coursecode[$i]',mark=AES_ENCRYPT('$mark
[$i]','$key'),grade='$grade[$i]',level='$level[$i]',year='$year[$i]' where
SerialNumber='$serialnumber[$i]'");
}
}
}
if(isset($_POST["saveBtn"])){
$studentid =$_POST['studentid'];
$serialnumber =($_POST['serialnumber']);
$countserialnumber =count($_POST['serialnumber']);
$coursecode =$_POST['coursecode'];
$mark =$_POST['mark'];

$level =$_POST['level'];
$year =$_POST['year'];
if ($studentid== '0' && $serialnumber== '0'&& $coursecode == '0' && $mark == '0'  &&
$year == '0' && $level == '0' ) {
echo "0";
} else {
$queries = array();
for ($i = 0; $i<$countserialnumber; $i++) {
if (!get_magic_quotes_gpc()) {
$coursecode[$i] = addslashes($coursecode[$i]);
$studentid[$i] = addslashes($studentid[$i]);
$serialnumber[$i] = addslashes($serialnumber[$i]);
$mark[$i] = addslashes($mark[$i]);
$hashmark[$i]=hash('sha3-224',$mark[$i]);
$year[$i] = addslashes($year[$i]);
$level[$i] = addslashes($level[$i]);
}
$queries[] =
"('$serialnumber[$i]','$studentid[$i]','$coursecode[$i]','$hashmark[$i]','$level[$i]','$year[$i]')"
;
$values = implode(", ", $queries);
$insert ="UPDATE hashedmarks SET
studentnumber='$studentid[$i]',coursecode='$coursecode[$i]',mark='$hashmark[$i]',level='$l
evel[$i]',year='$year[$i]' where SerialNumber='$serialnumber[$i]'";
$result = mysqli_query($link2,$insert) or die(mysqli_error($link2));
  }
  }
  }
if($update)
{
echo "Student results successfully published";
```

```
echo "<br>";
echo "
<br/> <a href='resultspublish.php'>Back</a></div>";
}
mysqli_close($link);
?>
```

RETRIEVE COURSE DETAILS
Retrievecoursedetails.php (script prints a PDF file of student course enrolment details)

```
<?
include 'config.php';
include 'auth.php';
include('config3.php');
$database = new Database();
extract ($_POST);
$studentid = $_SESSION['examnumber'];
if (!$link) {
die("Connection failed: " . mysqli_connect_error());
}
/* retrieve record */
$result = mysqli_query($link, "SELECT studentnumber, coursecode, level, year FROM test
where studentnumber='$studentid'");

$header = $database->runQuery("SELECT UCASE(`COLUMN_NAME`)
FROM `INFORMATION_SCHEMA`.`COLUMNS`
WHERE `TABLE_SCHEMA`='students'
AND `TABLE_NAME`='test'
and `COLUMN_NAME` in ('studentnumber','coursecode', 'level', 'year')");
require('fpdf/fpdf.php');
$pdf = new FPDF();
$pdf->AddPage();
$pdf->SetFont('Arial','B',16);
foreach($header as $heading) {
        foreach($heading as $column_heading)
                $pdf->Cell(54,12,$column_heading,1);
}
foreach($result as $row) {
        $pdf->Ln();
        foreach($row as $column)
                $pdf->Cell(54,12,$column,1);
}
$pdf->Output();
?>
```

RETRIEVE RESULTS
Studentfinalresults.php

```
<?
include 'config.php';
include 'config2.php';
include 'auth.php';
include 'config3.php';
include 'pk.php';
require('fpdf/fpdf.php');
$database = new Database();
extract ($_POST);
$studentnumber= $_SESSION['examnumber'];
$select="SELECT AES_DECRYPT(mark,'$key') FROM results WHERE studentnumber='$studentnumber'";
$result = mysqli_query($link, $select);
while($row = mysqli_fetch_assoc($result)){
	$mark = $row["AES_DECRYPT(mark,'$key')"];
	$hashmark=hash('sha3-224',$mark);
//
$query1 ="SELECT mark FROM hashedmarks WHERE mark='$hashmark'";
$check = mysqli_query($link2,$query1);
if(mysqli_num_rows($check)= =0) {

	echo "Could not retrieve your results. Please check with TEVETA";
	echo "<br>";
	echo "<a href='studentpage.php'>Back</a></div>";
	exit();

/* retrieve record */
}
else {
$result = mysqli_query($link, "SELECT results.studentnumber, results.coursecode, results.grade, results.level, results.year FROM results, studentdetails where studentdetails.studentnumber= results.studentnumber AND results.studentnumber='$studentnumber'");

$header = $database->runQuery("SELECT UCASE(`COLUMN_NAME`)
FROM `INFORMATION_SCHEMA`.`COLUMNS`
WHERE `TABLE_SCHEMA`='students'
AND `TABLE_NAME`='results'
and `COLUMN_NAME` in ('studentnumber','coursecode', 'grade', 'level', 'year')");
$pdf = new FPDF();
$pdf->AddPage();
// Page Header
$pdf->Image('images/logo.png',10,-1,70);
$pdf->SetFont('Arial','B',13);
// Move to the right
$pdf->Cell(80);
// Title
```

```
$pdf->Cell(80,10,'Statement of Results',1,0,'C');
// Line break
$pdf->Ln(20);

$pdf->SetFont('Times','B',12);
foreach($header as $heading) {
        foreach($heading as $column_heading)
                $pdf->Cell(45,12,$column_heading,1);
}
foreach($result as $row) {
        $pdf->Ln();
        foreach($row as $column)
                $pdf->Cell(45,12,$column,1);
}
$pdf->Output();
}
}
?>
```

MOBILE JAVA APPLICATION CODE

```
package mobilephone.ehc.novax.messenger;

import android.content.Context;
import android.content.Intent;
import android.content.SharedPreferences;
import android.os.Build;
import android.os.StrictMode;
import android.preference.PreferenceManager;
import android.support.annotation.RequiresApi;
import android.support.v7.app.AppCompatActivity;
import android.os.Bundle;
import android.support.v7.widget.LinearLayoutManager;
import android.support.v7.widget.RecyclerView;
import android.support.v7.widget.Toolbar;
import android.text.TextUtils;
import android.view.Menu;
import android.view.MenuInflater;
import android.view.MenuItem;
import android.view.View;
import android.view.inputmethod.InputMethodManager;
import android.widget.Button;
import android.widget.EditText;
import android.widget.ImageButton;
import android.widget.LinearLayout;
import android.widget.Toast;

import org.json.JSONArray;
import org.json.JSONException;
```

```
import org.json.JSONObject;

import java.io.IOException;
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.Statement;
import java.util.ArrayList;
import java.util.Date;
import java.util.List;

import mobilephone.ehc.novax.messenger.NetworkClasses.HttpURLConnectionExample;
import mobilephone.ehc.novax.messenger.dialogs.Server_pref_dialog;

public class MainActivity extends AppCompatActivity {

    private ImageButton sendButton; //Send Button
    private EditText PhoneNumber; //Phone Number
    private EditText MessageBody;  //Actual Message
    private RecyclerView recyclerView; //Message List Viewer
    private List<message> messages; //List Holding Messages
    private messageAdapter adapter; //Message Adapter
    private Toolbar toolbar; // App Toolbar
    private String body = ""; // Message body String



    //Initialize View Elements
    private void InitializeWidgets(){

        toolbar = findViewById(R.id.toolbar);
        setSupportActionBar(toolbar);
        getSupportActionBar().setTitle("Messenger");
        messages = new ArrayList<>();

        sendButton = findViewById(R.id.send_button);
        PhoneNumber = findViewById(R.id.phone_number_editText);
        MessageBody = findViewById(R.id.messageBody_editText);
        recyclerView = findViewById(R.id.MessageRecyclerView);
        recyclerView.setHasFixedSize(true);
        LinearLayoutManager layoutManager = new LinearLayoutManager(this);
        recyclerView.setLayoutManager(layoutManager);
    }


    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
```

```
        // Initialization Call
        InitializeWidgets();

        //Configure App Network Permission
        StrictMode.setThreadPolicy(new
StrictMode.ThreadPolicy.Builder().detectDiskReads().detectDiskWrites().detectNetwork().pe
naltyLog().build());

        //Button on Click
        sendButton.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {
                SharedPreferences                    preferences                    =
PreferenceManager.getDefaultSharedPreferences(MainActivity.this);
                String results_address = preferences.getString("server_results_address_pref", "");
                String details_address = preferences.getString("server_details_address_pref", "");
//                Toast.makeText(MainActivity.this, address, Toast.LENGTH_SHORT).show();

                //Get Phone Number from View
                String number = PhoneNumber.getText().toString().trim();
                //Get Message from View
                String message = MessageBody.getText().toString().trim();

                //Check if Phone Number View is not Empty
                if (TextUtils.isEmpty(number)) {
                    //Notify User about no phone Number
                    Toast.makeText(MainActivity.this,        "Enter        a        phone        Number",
Toast.LENGTH_SHORT).show();
                } else {

                    //Check if Number is 400 or 401
                    if (number.equals("400") || number.equals("401")){

                        try {
                            //Check if message string is not empty
                            if (!message.isEmpty()) {

                                //Split Message for field Extraction
                                String parts[] = message.split(" ");

                                //Check if Message length is within range
                                if (parts.length == 3){
                                    //Initialize Server Connection Interface
                                    HttpURLConnectionExample    httpURLConnectionExample    =    new
HttpURLConnectionExample();

                                    //Number entered is 400
                                    if (number.equals("400")){
                                        //Connect and Send Request to Server
```

```
                    httpURLConnectionExample.setPOST_URL(results_address,
                        parts[0],
                        parts[1],
                        parts[2]);

                    //Get Server response
                    String response =
httpURLConnectionExample.getResponseMessage();

                    //Parse the JSON response Array
                    JSONArray jsonarray = new JSONArray(response);
                    //Clear message Variable
                    body = "";

                    //Extract Elements From the Response
                    for (int i = 0; i < jsonarray.length(); i++) {

                       JSONObject jsonobject = jsonarray.getJSONObject(i);
                       String ExamNumber = jsonobject.getString("ExamNumber");
                       String CourseCode = jsonobject.getString("coursecode");
                       String Grade = jsonobject.getString("grade");
                       String Level = jsonobject.getString("level");
                       String Year = jsonobject.getString("year");

                       //Build Message
                       String buildFormat = "ExamNumber:" + ExamNumber + "\n" +
                            "Course Code:" + CourseCode + "\n" +
                            "Grade:" + Grade + "\n" +
                            "Level:" + Level + "\n" +
                            "Year:" + Year;

                       //Append Response Message to Message body
                       body = body + buildFormat + "\n\n";



                    }
                }
                //Number entered is 401
                if (number.equals("401")){
                    //Connect and Send Request to Server


                    httpURLConnectionExample.setPOST_URL(details_address,
                        parts[0],
                        parts[1],
                        parts[2]);

                    //Get Server response
```

```
                String response = httpURLConnectionExample.getResponseMessage();

                //Parse the JSON response Array
                JSONArray jsonarray = new JSONArray(response);
                //Clear message Variable
                body = "";

                //Extract Elements From the Response
                for (int i = 0; i < jsonarray.length(); i++) {
                   JSONObject jsonobject = jsonarray.getJSONObject(i);
                   String ExamNumber = jsonobject.getString("ExamNumber");
                   String CourseCode = jsonobject.getString("coursecode");
                   String Level = jsonobject.getString("level");
                   String Year = jsonobject.getString("year");

                   //Build Message
                   String buildFormat = "ExamNumber:" + ExamNumber + "\n" +
                         "Course Code:" + CourseCode + "\n" +
                         "Level:" + Level + "\n" +
                         "Year:" + Year;

                   //Append Response Message to Message body
                   body = body + buildFormat + "\n\n";
                }
             }



          }else{
             //Clear message Variable
             body = "";
             body = "Unknown Request";
          }
          //Append Message to View
          messages.add(new message(body, number));

          //Initialize Message Adapter
          adapter = new messageAdapter(MainActivity.this, messages);
          adapter.notifyDataSetChanged();
          //Apply Adapter to recycler view
          recyclerView.setAdapter(adapter);
          recyclerView.scrollToPosition(adapter.getItemCount() - 1);


       }

    } catch (JSONException e) {
       e.printStackTrace();
```

```
                } catch (IOException e) {
                    e.printStackTrace();
                }
            }
        }

        if (TextUtils.isEmpty(message)) {
            //Blank Message Warning
            Toast.makeText(MainActivity.this, "You are attempting to send an empty message " +
                    "body", Toast.LENGTH_SHORT).show();
        }


        Toast.makeText(MainActivity.this, "Sending to " + number, Toast.LENGTH_SHORT).show();


        LinearLayout mainLayout;

        mainLayout = findViewById(R.id.mainLinearLayout);

        InputMethodManager imm = (InputMethodManager)getSystemService(Context.INPUT_METHOD_SERVICE);
        imm.hideSoftInputFromWindow(mainLayout.getWindowToken(), 0);
      }



    });

  }

  @RequiresApi(api = Build.VERSION_CODES.HONEYCOMB)
  @Override
  public boolean onCreateOptionsMenu(Menu menu) {
    MenuInflater menuInflater = getMenuInflater();
    menuInflater.inflate(R.menu.preferences, menu);
    return super.onCreateOptionsMenu(menu);
  }

  @Override
  public boolean onOptionsItemSelected(MenuItem item) {

    int id = item.getItemId();

    switch (id)
    {

      case R.id.action_preferences:
```

```
            Server_pref_dialog serverPrefDialog = new Server_pref_dialog(this);
            serverPrefDialog.show();
            break;

        }
        return super.onOptionsItemSelected(item);
    }

}


package mobilephone.ehc.novax.messenger;

public class message {

    private String message;
    private String number;

    public message(String message, String number) {
        this.message = message;
        this.number = number;
    }
    public String getMessage() {
        return message;
    }
    public void setMessage(String message) {
        this.message = message;
    }
    public String getNumber() {
        return number;
    }
    public void setNumber(String number) {
        this.number = number;
    }
}


package mobilephone.ehc.novax.messenger;

import android.content.Context;
import android.support.v7.widget.RecyclerView;
import android.view.LayoutInflater;
import android.view.View;
import android.view.ViewGroup;
import android.widget.TextView;

import java.util.List;

public class messageAdapter extends
RecyclerView.Adapter<messageAdapter.messageViewHolder>{
```

```
    private Context ctx;
    private List<message> messages;

    public messageAdapter(Context ctx, List<message> messages) {
        this.ctx = ctx;
        this.messages = messages;
    }

    @Override
    public messageViewHolder onCreateViewHolder(ViewGroup parent, int viewType) {
        LayoutInflater inflater = LayoutInflater.from(ctx);
        View view = inflater.inflate(R.layout.mesage_layout, null);
        return new messageViewHolder(view);
    }

    @Override
    public int getItemCount() {
        return messages.size();
    }

    @Override
    public void onBindViewHolder(messageViewHolder holder, int position) {
        message message = messages.get(position);
        holder.message.setText(message.getMessage());
        holder.Recevingnumber.setText(message.getNumber());
    }

    class messageViewHolder extends RecyclerView.ViewHolder{

        TextView message;
        TextView Recevingnumber;

        public messageViewHolder(View itemView) {
            super(itemView);

            message = itemView.findViewById(R.id.MessageText);
            Recevingnumber = itemView.findViewById(R.id.receivingNumber);
        }
    }
}
```

Requestscript.php (retrieve results and encodes in json format for the mobile application)

```
<?php
$examnumber = ($_POST["examnumber"]);
$level = ($_POST["level"]);
$year = ($_POST["year"]);
```

```
include 'config.php';
include 'pk.php';
extract ($_POST);
if (!$link) {
die("Connection failed: " . mysqli_connect_error());
}
// block of code for decrypting results
$dbdata = array();
$result = mysqli_query($link, "SELECT studentnumber as ExamNumber, coursecode, grade, level, year FROM test where studentnumber='$examnumber' AND level ='$level' AND year ='$year'");
while ( $row = $result->fetch_assoc())  {
        $dbdata[]=$row;
  }
//Print array in JSON format
echo json_encode($dbdata);
?>
```

Requestscript1.php (retrieves course enrolment details and encodes it in json format for the mobile application)

```
<?php
$examnumber = ($_POST["examnumber"]);
$level = ($_POST["level"]);
$year = ($_POST["year"]);

include 'config.php';
extract ($_POST);
if (!$link) {
die("Connection failed: " . mysqli_connect_error());
}
// block of code for decrytping
$dbdata = array();
$result = mysqli_query($link, "SELECT studentnumber as ExamNumber, coursecode,level, year FROM test where studentnumber='$examnumber' AND level ='$level' AND year ='$year'");
while ( $row = $result->fetch_assoc())  {
        $dbdata[]=$row;
  }
//Print array in JSON format
echo json_encode($dbdata);
?>
```

Appendix 2: Field Questionnaire 1

The University of Zambia
School of Engineering

QUESTIONNAIRE ON CHALLENGES FACED BY TEVETA REGARDING DISSEMINATION OF EXAMINATION RESULTS
(TEVETA IT STAFF)

Web and Mobile Based Examination Results Dissemination and Verification System using Authenticated-Encryption: A Case of TEVETA

RESEARCHER
Lister Mseteka (2016145915)
Master of Engineering – ICT Security
0979 666312

Questionnaire No: …..

Dear Respondent,
I am a student at the University of Zambia in my final stage pursuing a Master of Engineering – ICT Security. I am conducting a baseline study to establish the challenges faced by TEVETA regarding dissemination of students' examination results.
You have been purposively sampled to provide the information. The information being collected is purely for academic purposes as such, it will be treated with maximum confidentiality.
Your co-operation will be greatly appreciated.

For any queries in relation to the survey, you may wish to contact the following:

Research Supervisors: Dr. Simon Tembo (simon.tembo@unza.zm) & Dr. Jackson Phiri (Jackson.phiri@cs.unza.zm)

Assistant Dean: Dr. Erastus Mwanaumo (erastus.mwanaumo@unza.zm)

INSTRUCTIONS:

1) You are encouraged to answer all questions to help us undertake a proper investigation on the challenges faced by TEVETA regarding dissemination of students' examination results.
2) Please express your opinion by indicating or ticking **(√)** your level of agreement / disagreement in the spaces or boxes provided.

SECTION A: DEMOGRAPHIC DATA

1) **Sex:** (a) Male ☐ (b) Female ☐

2) **Age in years.**

(a) 18 – 22 ☐ (c) 30 – 34 ☐
(b) 22 – 26 ☐ (d) 34 and above ☐

3) Present job title or position

(a) Data Entry Associate ☐
(b) Systems Developer/Programmer ☐
(c) Other (Specify)……..

4) Professional qualifications

(a) Masters Degree ☐
(b) Bsc Computer Science/Computing ☐
(c) Diploma in Computer Studies/IT ☐
(d) Other (specify) ……

5) Years of experience in your profession:

(a) 1 – 5 ☐ (b) 5 – 9 ☐ (c) 9 and above ☐

SECTION B: TEVETA EXAMINATION CYCLE

The diagram in figure 1 shows the current business processes for TEVETA examination cycle.

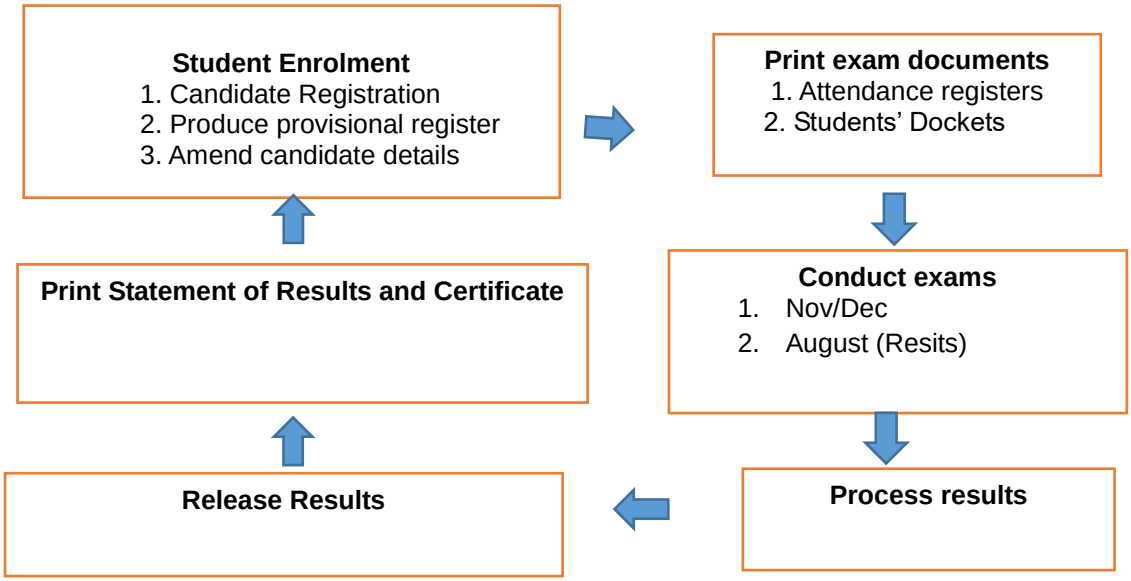


Figure 1: Teveta examination cycle

1) Do you face challenges in candidate enrolment for examinations?

(a) Yes ☐ (b) No ☐

2) What challenges do you face in candidate enrolment for examinations? Tick (√) all that you think apply in the boxes provided.

(i) Large number of candidates ☐
(ii) Few personnel in data entry ☐
(iii) Omission of candidates ☐
(iv) Errors in data entry ☐
(v) Registration of illegal candidates ☐
(vi) Inaccurate subject entries by candidates ☐
(vii) Incomplete registration forms ☐
(viii) Incorrect examination numbers resulting in duplicate entries ☐
(ix) Disparities in the number of students registered for examinations between Training Institutions and TEVETA ☐
(x) Registration forms received late ☐
(xi) Failure by students to verify their details ☐
(xii) TEVETA system (application) failure to capture all candidates ☐
(xiii) TEVETA system (application) is slow ☐
(xiv) Other (indicate)……

3) Recommend solutions that would reduce or eradicate challenges in candidate enrolment for examination. Tick (√) all that you think apply in the boxes provided

i. Online registration for examinations through a mobile or web based application ☐
ii. Online verification of candidate details through a mobile or web based application ☐
iii. Recruit more personnel ☐
iv. Update the TEVETA system regularly ☐
v. Other (indicate)…….

4) What problems do you face in students' examination results entry, processing, storage and management?

i. Incorrect marks calculated due to rigorous calculations ☐
ii. Incorrect marks entered due to human error ☐
iii. Data processing errors in the TEVETA examinations IT system (application) ☐
iv. Students examination results are stored in plain text without encryption hence can be viewed by anyone as long as they have access to the database ☐
v. Mismanagement of students' data that result in incorrect updates or data loss ☐
vi. Other (indicate)…….

5) What do you think are the factors that contribute to the delay in releasing examination results for TEVETA examined students? Tick (√) all that you think apply in the boxes provided.

i. Large number of students ☐
ii. Rigorous calculations of marks ☐
iii. Few Personnel ☐
iv. TEVETA system (application) is slow ☐
v. Long and tedious administrative procedures before students' examination results are released to the public ☐
Other (indicate)…….

6) Do you think a mobile application will improve dissemination of examination results?

(a) Yes ☐ (b) No ☐ (c) Not Sure ☐

7) What feature would you want to see if a mobile application is developed for dissemination of students' examination results?

(i) Allow candidates to enrol for examinations using a mobile phone ☐
(ii) Allow candidates to verify their details ☐
(iii) Allow candidates to view their details ☐
(iv) Able to detect illegal students ☐
(v) Eradicate wrong subject entries ☐
(vi) Eradicate multiple registrations by the same candidate ☐
(vii) Secure storage of candidate enrolment and examination results data ☐
(viii) Allow students to view results ☐
(ix) Other (indicate)…….

8) Do you think a web examination results dissemination system will improve dissemination of examination results?

(a) Yes ☐ (b) No ☐ (c) Not sure ☐

9) What features would you want to see if a web based examination results dissemination system is developed?

(i) Allow candidates to enrol for examinations online ☐
(ii) Allow candidates to view their enrolment details online ☐
(iii) Allow candidates to verify their enrolment details online ☐
(iv) Able to detect illegal students ☐
(v) Eradicate wrong subject entries ☐
(vi) Eradicate multiple registrations by the same candidate ☐
(vii) Secure storage of candidate enrolment and examination results data ☐
(viii) Able to deter unauthorised amendments to examination results ☐
(ix) Allow students to view results online ☐
(x) Other (indicate)…….

THANK YOU FOR YOUR TIME

Appendix: Field Questionnaire 2

The University of Zambia
School of Engineering

QUESTIONNAIRE ON CHALLENGES FACED BY STUDENTS REGARDING ACCESS TO TEVETA EXAMINATION RESULTS
(TEVETA EXAMINED STUDENTS)

A Web and Mobile Based Examination Results Dissemination and Verification System using Authenticated-Encryption: A Case of TEVETA

RESEARCHER
Lister Mseteka (2016145915)
Master of Engineering – ICT Security
0979 6663

Questionnaire No: …..

Dear Respondent,
I am a student at the University of Zambia in my final stage pursuing a Master of Engineering – ICT Security. I am conducting a baseline study to establish the challenges faced by students regarding access to TEVETA examination results.
You have been purposively sampled to provide the information. The information being collected is purely for academic purposes as such, it will be treated with maximum confidentiality.

Your co-operation will be greatly appreciated.

For any queries in relation to the survey, you may wish to contact the following:

Research Supervisors: Dr. Simon Tembo (simon.tembo@unza.zm) & Dr. Jackson Phiri (Jackson.phiri@cs.unza.zm)

Assistant Dean: Dr. Erastus Mwanaumo (erastus.mwanaumo@unza.zm)

INSTRUCTIONS:

1) You are encouraged to answer all questions to help us undertake a proper investigation on the challenges faced by students regarding access to examination results.

2) Please express your opinion by indicating or ticking **(√)** your level of agreement / disagreement in the spaces or boxes provided.

SECTION A: DEMOGRAPHIC DATA

3) **Sex:** (a) Male ☐ (b) Female ☐

4) **Age in years.**

(a)	14 – 18	☐	(d) 26 – 30	☐
(b)	18 – 22	☐	(e) 30 – 34	☐
(c)	22 – 26	☐	(f) 34 and above	☐

5) **Marital status**

(a)	Single	☐	(d) Separated	☐
(b)	Married	☐	(e) Divorced	☐
(c)	Widowed	☐		

6) **Institution of Study**

(a)	College	☐	(c)Trades Training Institute	☐
(b)	Training Centre	☐		

7) **Name of Institution**

……

8) **Programme of Study**

(a)	Diploma	☐	(c) Trade Test Certificate	☐
(b)	Craft Certificate	☐		

SECTION B: TEVETA SYSTEM

1) How long does it take for TEVETA to release examination results after sitting for them?

(a) After two months ☐ (c) It varies ☐

(b) After three months ☐

2) **How long does it take for you to know your examination results after they are released?**

(a) Within a day ☐ (c) After some weeks

(b) After some days ☐ (d) After some months ☐

3) **Are you allowed to proceed to the next level of study before results are released?**

(a) Yes ☐ (b) No ☐

4) **If your answer is No to question 3, does it affect syllabi coverage taking into account the fact that the TEVET academic calendar remains fixed regardless of when examination results are released?**

(a) Yes ☐ (b) No ☐

5) **If the answer to question 4 is yes, what measures does your training institution put in place to ensure that you finish the syllabi?**

……..

SECTION C: ICT

1) What mobile service provider is available in your area?

a) Airtel ☐ b) ZAMTEL ☐ c) MTN ☐

d) No cellular network ☐

2) Do you have a mobile phone?

a) Yes ☐ b) No ☐

3) What make of mobile phone are you using?

Please specify …….

4) What services are available on your mobile phone?

a) Call and send SMS's only ☐ b) Internet service ☐ c) WhatsApp ☐

5) Do you think a mobile application will improve access to examination results?

(a) Yes ☐ (c) Not Sure ☐
(b) No ☐

6) Do you have access to the internet

(a) Yes ☐ (b) No ☐

7) How do you access the internet?

(a) Internet Cafe ☐
(b) Mobile Device (e.g. mobile phone, tablet) ☐
(c) Institution of Study (e.g. College, Training Centre, Trades Training Institute) ☐
(d) Public Wifi (e.g. shopping mall) ☐
(e) Dongle ☐

8) Do you think a web examination results dissemination system will improve access to examination results?

(a) Yes ☐ (c) Not Sure ☐
(b) No ☐

SECTION D: PAYMENTS

1) **Do you face challenges with the current payment system for TEVETA registration and examination fees?**

   a) Yes ☐ b) No ☐

2) **What challenges do you face with the current payment system for TEVETA registration and examination fees?**

   a) Long queues at the bank ☐
   b) Omission of candidate payment details by institution of study to TEVETA ☐
   c) Other (indicate)……

3) **Do you have a bank account?**

   Yes ☐ No ☐

4) **Indicate the name of the bank you have an account with**
   ……

5) **Do you think a mobile bank transfer from your account to TEVETA would resolve problems of omission of candidate payment details by institutions of study and long bank queues?**

   a) Yes ☐ b) No ☐

   b) Other (indicate) ……..

THANK YOU FOR YOUR TIME

Appendix: Field Questionnaire 3

The University of Zambia
School of Engineering

QUESTIONNAIRE ON CHALLENGES FACED BY TEVETA REGARDING DISSEMINATION OF EXAMINATION RESULTS
(EXAMINATIONS OFFICERS & STAFF IN CHARGE OF EXAMINATIONS IN TEVETA EXAMINED INSTITUTIONS)

Web and Mobile Based Examination Results Dissemination and Verification System using Authenticated-Encryption: A Case of TEVETA

RESEARCHER
Lister Mseteka (2016145915)
Master of Engineering – ICT Security
0979 666312

Questionnaire No: …..

Dear Respondent,
I am a student at the University of Zambia in my final stage pursuing a Master of Engineering – ICT Security. I am conducting a baseline study to establish the challenges faced by TEVETA regarding dissemination of students' examination results.
You have been purposively sampled to provide the information. The information being collected is purely for academic purposes as such, it will be treated with maximum confidentiality.
Your co-operation will be greatly appreciated.

For any queries in relation to the survey, you may wish to contact the following:

Research Supervisors: Dr. Simon Tembo (simon.tembo@unza.zm) & Dr. Jackson Phiri (Jackson.phiri@cs.unza.zm)

Assistant Dean: Dr. Erastus Mwanaumo (erastus.mwanaumo@unza.zm)

INSTRUCTIONS:

1) You are encouraged to answer all questions to help us undertake a proper investigation on the challenges faced by TEVETA regarding dissemination of students' examination results.
2) Please express your opinion by indicating or ticking **(√)** your level of agreement / disagreement in the spaces or boxes provided.

SECTION A: DEMOGRAPHIC DATA

1) Sex: (a) Male ☐ (b) Female ☐

2) Age in years.

(a) 18 – 22 ☐ (c) 30 – 34 ☐
(b) 22 – 26 ☐ (d) 34 and above ☐

3) Present job title or position

(a) Examinations Officer ☐
(b) Assistant Examinations Officer ☐
(c) Other (Specify)……

4) Professional qualifications

(e) Masters Degree ☐ (b) Degree ☐
(c) Diploma ☐

5) Years of experience in your profession:

(a) 1 – 5 ☐ (b) 5 – 9 ☐ (c) 9 and above ☐

SECTION B: TEVETA SYSTEM

1) The diagram in figure 1 shows the current business processes for TEVETA examination cycle. **Question 1.1 – 1.4 are based on figure 1**

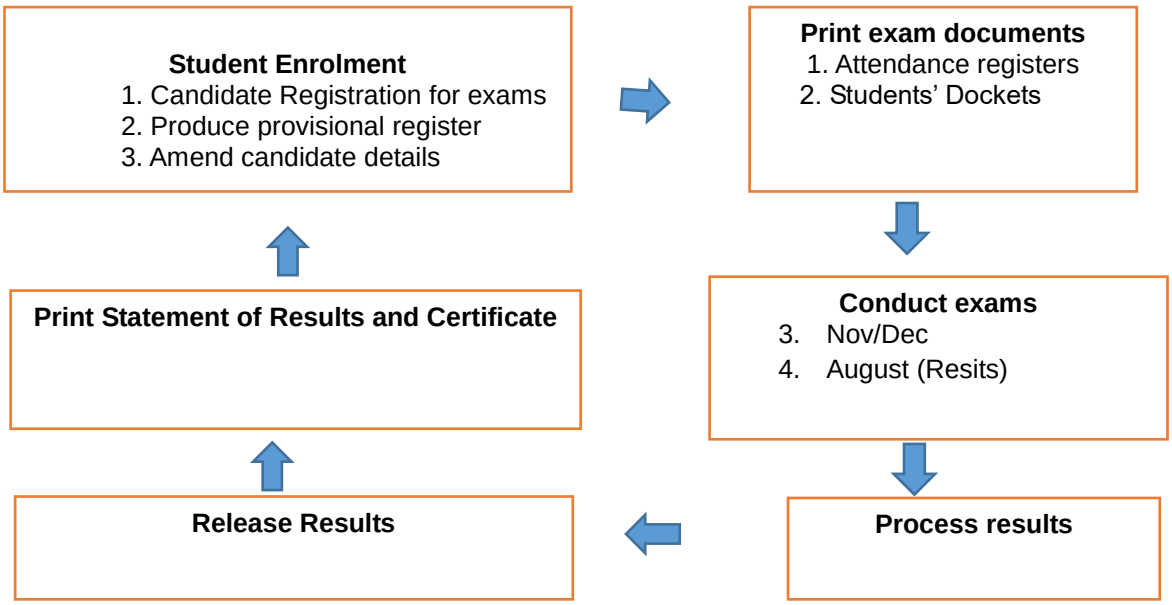


Figure 1: Teveta examination cycle

1.1 Do you face challenges in candidate enrolment for examinations?

(b) Yes ☐ (b) No ☐

1.2 What challenges do you face in candidate enrolment for examinations? Tick (√) all that you think apply in the boxes provided.

(i) Large number of candidates ☐
(ii) Few personnel in data entry ☐
(iii) Omission of candidates on the spreadsheet sent to TEVETA ☐
(iv) Errors in data entry ☐
(v) Registration of illegal candidates ☐
(vi) Inaccurate subject entries by candidates ☐
(vii) Incomplete registration forms ☐
(viii) Incorrect examination numbers resulting in duplicate entries ☐
(ix) Disparities in the number of students registered for examinations between Training Institutions and TEVETA ☐
(x) Registration forms received late ☐
(xi) Failure by students to verify their details ☐
(xii) Non submission of registration forms by students ☐
(xiii) Other(indicate)……
….

1.2 Recommend solutions that would reduce or eradicate challenges in candidate enrolment for examination. Tick (√) all that you think apply in the boxes provided

(i) Online registration for examinations through a mobile or web based application ☐
(ii) Online verification of candidate details through a mobile or web based application ☐
(iii) Recruit more personnel ☐
(iv) Other(indicate)……

1.3 What do you think are the factors that contribute to the delay in releasing examination results for TEVETA examined students? Tick (√) all that you think apply in the boxes provided.

(i) Large number of students ☐
(ii) Rigorous calculations of marks ☐
(iii) Few Personnel ☐
(iv) Long and tedious administrative procedures before students' examination results are released to the public ☐
(v) Other(indicate)……

2) **Do you think a mobile application will improve candidate enrolment for examinations?**

(a) Yes ☐ (b) No ☐ (c) Not Sure ☐

3) **What feature would you want to see if a mobile application is developed for candidate enrolment of examinations?**

(i) Allow candidates to enrol for examinations ☐
(ii) Allow candidates to verify their details ☐
(iii) Allow candidates to view their details ☐
(iv) Reject enrolment for examination by illegal candidates ☐
(v) Reject wrong subject entries by candidate ☐
(vi) Reject multiple registrations by the same candidate ☐
(vii) Other(indicate)……

4) **Do you think a web examination results dissemination system will improve dissemination of examination results?**

(a) Yes ☐ (b) No ☐ (c) Not sure ☐

5) **What features would you want to see if a web based examination results dissemination system is developed?**

(i) Allow candidates to enrol for examinations online ☐
(ii) Allow candidates to view their enrolment details online ☐
(iii) Allow candidates to verify their enrolment details online ☐
(iv) Reject enrolment for examination by illegal candidates ☐
(v) Reject wrong subject entries by candidate ☐
(vi) Reject multiple registrations by the same candidate ☐
(vii) Other(indicate)……

THANK YOU FOR YOUR TIME

Appendix: Field Questionnaire 4

The University of Zambia
School of Engineering

QUESTIONNAIRE ON CHALLENGES FACED BY TEVETA REGARDING DISSEMINATION OF EXAMINATION RESULTS
(TEVETA IT STAFF)

Web and Mobile Based Examination Results Dissemination and Verification System using Authenticated-Encryption: A Case of TEVETA

RESEARCHER
Lister Mseteka (2016145915)
Master of Engineering – ICT Security
0979 666312

Questionnaire No: …..

Dear Respondent,
I am a student at the University of Zambia in my final stage pursuing a Master of Engineering – ICT Security. I am conducting a baseline study to establish the challenges faced by TEVETA regarding dissemination of students' examination results.
You have been purposively sampled to provide the information. The information being collected is purely for academic purposes as such, it will be treated with maximum confidentiality.
Your co-operation will be greatly appreciated.

For any queries in relation to the survey, you may wish to contact the following:

Research Supervisors: Dr. Simon Tembo (simon.tembo@unza.zm) & Dr. Jackson Phiri (Jackson.phiri@cs.unza.zm)

Assistant Dean: Dr. Erastus Mwanaumo (erastus.mwanaumo@unza.zm)

INSTRUCTIONS:

1) You are encouraged to answer all questions to help us undertake a proper investigation on the challenges faced by TEVETA regarding dissemination of students' examination results.
2) Please express your opinion by indicating or ticking **(√)** your level of agreement / disagreement in the spaces or boxes provided.

SECTION A: DEMOGRAPHIC DATA

1) Sex: (a) Male ☐ (b) Female ☐

2) Age in years.

(a) 18 – 22 ☐ (c) 30 – 34 ☐
(b) 22 – 26 ☐ (d) 34 and above ☐

3) Present job title or position

……..

4) Professional qualifications

(f) Masters Degree ☐ (b) Bsc Computer Science/Computing ☐
(c) Diploma in Computer Studies/IT ☐

5) Years of experience in your profession:

(a) 1 – 5 ☐ (b) 5 – 9 ☐ (c) 9 and above ☐

SECTION B: INFORMATION SECURITY AUDIT

1) Does your institution have an information security policy?

   Yes ☐ No ☐

2) Does your institution have an information security policy that is appropriate, based on industry standards such as ISO/IEC 27001:2005?

   Yes ☐ No ☐

3) Is there a formal user registration process assigning and revoking access rights to systems and services?

   Yes ☐ No ☐

4) Are user access rights regularly reviewed, and removed upon termination of employment?

   Yes ☐ No ☐

5) Are human resources subject to online screening?
   Yes ☐ No ☐

6) Do human resources have terms and conditions of employment defining their information security responsibilities?

   Yes ☐ No ☐

7) Are employees required to adhere to the information security policies and procedures, provided with awareness, education and training, and is there a disciplinary process?

   Yes ☐ No ☐

8) Are there procedures for the removal, disposal and transit of media containing information?

   Yes ☐ No ☐

9) Do all devices that store or process students' examination results utilize antimalware with the current signature files?

   Yes ☐ No ☐

10) Do all devices that store or process students' examination results have access control that is configured on a least privilege model (a person only has access to the device/data that they need)?

    Yes ☐ No ☐

11) Do all devices that store or process students' examination results at a minimum have vulnerability scanning performed at least monthly?

    Yes ☐ No ☐

12) Do all devices that store or process students' examination results at a minimum have all unnecessary ports and services disabled and the devices used for limited functions (e.g. A device acting solely as a file server vs. a file server, FTP server, and web server)?

Yes ☐ No ☐

13) Do all mobile devices (e.g. smartphones, tablets) that store students' examination results at a minimum have access control to the device (complex password to access device)?

Yes ☐ No ☐

14) Are all devices that store students' examination results encrypted?

Yes ☐ No ☐

15) Is there a policy for the use of cryptography and key management?

Yes ☐ No ☐

16) Are information, software and systems subject to back up and regular testing?

Yes ☐ No ☐

17) Are there controls in place to log events and generate evidence?

Yes ☐ No ☐

18) Does your firm perform industry standard logging and monitoring on devices that store or process students' examination results?

Yes ☐ No ☐

THANK YOU FOR YOUR TIME