

**IMPROVED MECHANISM FOR DETECTING EXAMINATIONS
IMPERSONATIONS IN PUBLIC HIGHER LEARNING INSTITUTIONS;
CASE OF THE MWALIMU NYERERE MEMORIAL ACADEMY (MNMA)**

DOMITION JASSON LWANGISA

**A DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF MASTERS OF SCIENCE IN
COMPUTER SCIENCE**

**DEPARTMENT OF MATHEMATICS, INFORMATION AND
COMMUNICATION TECHNOLOGY**

OF THE OPEN UNIVERSITY OF TANZANIA

2025

CERTIFICATION

The undersigned certifies that he has read and here by recommends for acceptance by The Open University of Tanzania a dissertation entitled, **“Improved Mechanism for Detecting Examinations Impersonations in Public Higher Learning Institutions; Case of the Mwalimu Nyerere Memorial Academy”**. In partial fulfillment of the requirements for the award of Degree of Masters of Science in Computer Science (MSCS).

.....

Dr. Rogers Philip Bhalalusesa

(Supervisor)

.....

Date

.....

Dr. Selemani Ismail

(Supervisor)

.....

Date

COPYRIGHT

No part of this Dissertation may be reproduced, stored in any retrieval system, or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the author or The Open University of Tanzania in that behalf.

DECLARATION

I, **Domition Jasson Lwangisa**, declare that, the work presented in this dissertation is original. It has never been presented to any other University or Institution. Where other people's works have been used, references have been provided. It is in this regard that I declare this work as originally mine. It is hereby presented in partial fulfilment of the requirement for the Degree of Masters of Science in Computer Science (MSCS).

.....

Signature

.....

Date

ACKNOWLEDGEMENT

I extend my sincerest thanks to my supervisor, Dr. Rogers Bhalalusesa for his firm supervision, fruitful advice, and continuous support during this study. His expertise, encouragement, and patience have been helpful in modeling this report. I am also grateful to the faculty members of the Department of Mathematics, Information and Communication Technology for their insightful comments and suggestions, which have enhanced the value of this study. Special thanks are due to Dr. Khamis Kalegele, Dr. Ernest Haonga and Mr. Adam Charles for their assistance and encouragement.

I extend my appreciation to my friends and family for their considerate, inspiration, and solid trust in my capacities. Their good support strengthened and encouraged me during difficult times. Additionally, I would like to recognize the assistance provided by Alphaxsad Kakulu, Dr. Sixbert Msambichaka, Diana Mdope and Denis Malele for their contributions to data collection and analysis.

Finally, I am appreciative to the respondents for their readiness to participate and share their insights, without which this research would not have been possible.

ABSTRACT

Student identification documents, such as ID cards and exam hall tickets, are crucial for verifying exams eligibility in public higher learning institutions. However, these methods have security vulnerabilities, including weak authentication, lack of encryption, and inadequate anti-counterfeiting measures, making impersonation easier. The study focused on enhancing the detection of impersonations in physical examinations in Public Higher Learning Institutions. The main goal was to develop an improved mechanism for detecting impersonations, with specific objectives to identify key technologies, design an enhanced Natural Language Processing (NLP) model, and evaluate the developed model. The research was conducted at the Mwalimu Nyerere Memorial Academy (MNMA) due to its current high enrollment rate with low number of academics, involving 525 respondents including academic staff, ICT officers, and students. A mixed research methodology was adopted, the study used a case study approach with stratified sampling, employing semi-structured interviews, document analysis, and surveys for data collection. The study analyzed data using content analysis, statistics, and probability theory, presenting findings through graphs and UML diagrams. It developed an enhanced NLP model with Laravel, Flutter, and MySQL, integrating QR codes for student authentication through dynamic question generation. Results confirmed model efficiency in improving security and verification with minimal time and cost.

Keywords: *Impersonations, Examinations, Higher Learning Institution, Impersonations detection, impersonator, Dynamic Challenging questions, QR Code and NLP Model.*

TABLE OF CONTENTS

CERTIFICATION	ii
COPYRIGHT	iii
DECLARATION.....	iv
ACKNOWLEDGEMENT.....	v
ABSTRACT	vi
ABSTRACT	vi
LIST OF TABLES	xvi
LIST OF FIGURES	xvii
LIST OF ABBREVIATIONS AND ACRONYMS	xix
CHAPTER ONE	1
INTRODUCTION.....	1
1.1 Introduction.....	1
1.2 Background of the Study	2
1.3 Statement of the Research Problem	5
1.4 Research Objectives.....	6
1.4.1 General Research Objective.....	6
1.4.2 Specific Research Objectives.....	7
1.5 Research Questions	7
1.5.1 Specific Research Questions.....	7
1.6 Relevance of the Research	8
CHAPTER TWO	9
LITERATURE REVIEW.....	9
2.1 Overview.....	9

2.2	Conceptual Definitions	9
2.3	Critical Review of a Supporting Theory	11
2.4	The Theory of Human Identification	13
2.4.1	Bases for Formal Identification	15
2.4.1.1	Names as a base of identification	15
2.4.1.2	Codes	16
2.4.1.3	Knowledge-Based Identification	17
2.4.1.3.1	Banking	19
2.4.1.3.2	Healthcare Systems	19
2.4.1.3.3	Online Services and E-commerce	19
2.4.1.3.4	Government Services	20
2.4.1.3.5	Education Systems	20
2.4.1.3.6	Summary	20
2.4.1.4	Token-Based Identification	21
2.4.1.5	Biometrics	21
2.5	Empirical Analysis of Relevant Studies	22
2.5.1	Current Techniques for Detecting Impersonations during Traditional-In-Class Examinations	23
2.5.2	Impersonations Detection Mechanisms Related to this Study	31
2.6	Research Gap	34
2.7	Focus of the Research	35
2.8	A conceptual framework of an Improved Mechanism for Detecting Traditional-in-Class Examinations Impersonations in Tanzania Public Higher Learning Institutions.	36

CHAPTER THREE	37
RESEARCH METHODOLOGY	37
3.1 Overview	37
3.2 Research Strategy	37
3.3 Study Area	39
3.4 Study Population	40
3.5 Sample Design	41
3.6 A Methodology for Developing an Enhanced NLP Model Which Detects Examinations Impersonations in PHLIS.....	42
3.7 Research Design	46
3.8 Data Collection Methods	47
3.8.1 Data Collection Methods	47
3.8.1.1 Semi-structured Interview.....	47
3.8.1.2 Survey Questionnaire.....	48
3.8.1.3 Secondary Data	50
3.8.1.4 Demonstration.....	50
3.9 Data Quality Control Management.....	50
3.9.1 Pre-Test.....	51
3.9.2 Triangulation.....	51
3.9.3 Ethical Considerations	51
3.9.4 Rigorousness	52
3.10 Data Analysis and Presentation	52
3.11 Performing Usability Test of the Developed Mechanism for Detecting Examinations Impersonations	53

3.12	Summary	54
CHAPTER FOUR.....		55
FINDINGS AND DISCUSSION		55
4.1	Introduction.....	55
4.2	Socio-Demographic Attributes of the Respondents.....	56
4.2.1	Age of Respondents	56
4.2.2	Education Level of Respondents	58
4.3	Academics’ Awareness and Perception on the Concept of Impersonations	59
4.4	Prominent Impersonations Detection Technologies in Traditional-In- Class Examinations in Public Higher Learning Institutions	60
4.4.1	Methods Used to Collect Information from Academics and ICT Officers Regarding Prominent Impersonations Detection Technologies	61
4.4.2	Respondents’ Knowledge and Understanding on Impersonations Detection Technologies	62
4.4.3	Prominent Technologies for Detecting Impersonations in the Context of Traditional –in-Class Examinations in Tanzania Public Higher Learning Institutions	63
4.4.3.1	Facial Recognition Technology	65
4.4.3.2	Biometric Authentication Systems	65
4.4.3.3	Behavioral Analytics Tools	66
4.4.3.4	Proctoring Software Platforms.....	66
4.4.3.5	Dynamic Challenging Questions Based on Student’s Profiles	66

4.4.4	Discussion	67
4.4.5	Summary	67
4.5	Developing an Enhanced Natural Language Processing (NLP) Model for Detecting Impersonations in the Context of Traditional-In-Class Examinations in Tanzania Higher Learning Institutions	68
4.5.1	Introduction.....	68
4.5.2	Identifying Suitable Mechanism (Technique) for Detecting Impersonations in Traditional-in-class Examinations in Tanzania Public Higher Learning Institutions	69
4.5.3	Proposed System Architecture of the Improved Mechanism for Detecting Impersonations in Traditional-In-Class Examinations in Tanzania Public Higher Learning Institutions	72
4.5.4	Summary	76
4.5.5	Designing the Enhanced NLP Model for Generating Dynamic Challenging Questions Based on Student's Profile.....	77
4.5.5.1	Implementing the Proposed Enhanced NLP Model for Detecting Examinations Impersonations as Shown in Figure 4.6.....	79
4.5.5.1.1	User Enrollment.....	80
4.5.5.1.2	QR Code Generation.....	80
4.5.5.1.3	Authentication Process	81
4.5.5.1.4	Feature Extraction.....	81
4.5.5.1.5	Model Training	82
4.5.5.1.6	Template Design	82
4.5.5.1.7	Evaluation	82

4.5.5.1.8	Dynamic Challenging Questions (DCQNS) Presentations.....	82
4.5.5.1.9	Impersonation Detection.....	82
4.5.5.1.10	Summary	84
4.5.5.2	A mathematical Representation on the Technique for Generating Dynamic Challenging Questions	85
4.5.5.3	System Describing the Working Mechanism of the Enhanced NLP Model	87
4.5.5.4	Use Case Diagram of the Proposed Improved Impersonations Detection System	91
4.5.5.5	Database Design of the Proposed Impersonations Detection System ..	91
4.5.5.6	Sequence Diagram of the Proposed Improved Impersonations Detection System	98
4.5.6	Description of the Main Operations Presented in Figure 4.7	101
4.5.7	Designing Impersonation Detection System Based on NLP Model...	104
4.5.8	Selected Frameworks for the Implementation of the Proposed NLP Model for Detecting Impersonations in Traditional-In-Class Examinations (system).....	106
4.5.8.1	Implementation of the Mobile Application Client Side.....	107
4.5.8.2	Implementation of the Web Server Side	109
4.5.8.3	Generation of QR codes.....	111
4.5.8.4	Summary	112
4.5.9	The Actual Implementation of Core Parts of the Proposed Impersonations Detection System (Coding)	113
4.5.9.1	Codes for Scanning Student' QR code	113

4.5.9.2	Generating Dynamic Challenging Questions (DCQNs) based on Student Profile	113
4.5.9.3	Confirming Students Attendance	114
4.5.9.4	Confirming and Reporting Impersonations	114
4.5.9.5	Implementing user Login Page (Administrator Page and other System Users) on the Web Application.....	114
4.5.9.6	Implementing user Login Page (Administrator Page and other Susers) on the Mobile Application (Invigilator Only).....	114
4.5.9.7	Adding New Examination to the Database	114
4.5.9.8	Assigning Students to an Examination	115
4.5.9.9	Adding Students to the Database (Students Registration)	115
4.5.9.10	Adding Invigilators to the Database (Invigilators Registration).....	115
4.5.10	The Major User Interfaces from the Proposed Improved Impersonations Detection System	115
4.6	Evaluating the Proposed Improved Impersonations Detection Model	116
4.6.1	Students Registration	117
4.6.2	Usability Assessment of the Proposed Impersonation Detection Mechanism.....	118
4.6.2.1	Results from System' Usability Assessment	119
4.6.3	Efficiency of Generating Dynamic Challenging Questions Based on Students' Profile Along with their Corresponding Answers	120
4.6.4	Performing a Response Time Acceptance Testing	122

4.6.5	Performing some Analysis to Test the System's Reliability and Accuracy	125
4.6.5.1	False Rejection.....	125
4.6.5.2	False Rejection Rate (FRR)	127
4.6.5.3	False Acceptance (FA).....	127
4.6.5.4	False Acceptance Rate (FAR).....	129
4.6.5.5	Convenience.....	129
4.6.5.5.1	Adaptive Question Difficulty.....	130
4.6.5.5.2	QR code Reliability	130
4.6.5.5.3	Feedback Mechanism	130
4.6.5.5.4	Summary	131
4.6.5.6	Security	131
4.6.6	Deployment of the Proposed IMDIs System	131
4.7	Significance of this Study	132
4.7.1	Enhanced Security and Verification	133
4.7.2	Streamlined Administrative Processes.....	133
4.7.4	Increased Student Engagement and Satisfaction	133
4.7.5	Support for Remote and Online Learning.....	134
4.7.6	Compliance with Regulatory Standards	134
4.7.7	Innovation in Educational Technology.....	134
CHAPTER FIVE.....		136
CONCLUSION AND RECOMMENDATIONS.....		136
5.1	Conclusion	136
5.2	Recommendations and Future Works.....	139

REFERENCES.....	141
APPENDICES	158

LIST OF TABLES

Table 3.1:	The Population of academics at the MNMA	41
Table 3.2:	Population of ICT staff at the MNMA.....	41
Table 3.3:	The Number of Respondents	42
Table 4.1:	Distribution of Respondents (Academics) by Age	58
Table 4.2:	Distribution of Respondents (Students) by Age	58
Table 4.3:	Education Level of Academics (n=130)	59
Table 4.4:	Education Level of ICT Officers (n=5)	59
Table 4.5:	Prominent Technologies for Detecting Impersonations in the Context of Traditional –in-class Examinations in Tanzania Public Higher Learning Institutions Identified by Academics (n=140)	64
Table 4.6:	Academics Responses on the Improved Impersonations Detection Approaches	72
Table 4.7:	ICT Officers Responses on Impersonations Detection Approaches.....	72
Table 4.8:	Results from Authenticating and Verifying Gstudents.....	119
Table 4.9:	Impersonators Responses and Percentages of Correct Answers During Authentication and Verification of their Identities	119
Table 4.10:	Analysis of the Efficiency of Generating Dynamic Challenging Questions Based on Student Profile.....	122
Table 4.11:	Result of the Test Carried out on the System	127
Table 4.12:	Result of the Test Carried out on the System.	129

LIST OF FIGURES

Figure 2.1:	Context-Aware E-Examination Architecture Framework.....	32
Figure 2.2:	A conceptual framework of an improved mechanism for detecting Traditional-in-class Examinations Impersonations in Tanzania Public higher Learning Institutions	36
Figure 3.1:	The Prototyping System Development Methodology	44
Figure 4.1:	Impersonations Awareness Among Academics	60
Figure 4.2:	Respondents' Knowledge and Understanding on Impersonations Detection Technologies.	62
Figure 4.3:	Respondents' Responses to the Institution Syndicate where Impersonations are Reported.....	74
Figure 4.4:	Academics Response on Witnessing Action Tendered by an Impersonator that Aimed at Harming the Invigilator	76
Figure 4.5:	Development of the Proposed Improved Impersonations Detection System	79
Figure 4.6:	Phases for the Proposed Enhanced NLP Model for Detecting Examinations Impersonations	83
Figure 4.7:	A Conceptual Design Showing how to Use the Proposed Impersonation Detection system	90
Figure 4.8:	Use-Case Diagram of the Proposed System for Detecting Impersonations in Traditional-in-Class Examinations in THLIS.....	91
Figure 4.9:	Entity Relationship Diagram (ERD-models) of the Proposed System	98
Figure 4.10:	A Sequence Diagram in the Event of Fake Identity Fard/QR Code	

	and Impersonations Detection	99
Figure 4.11:	A Sequence Diagram in the Event of Presenting Valid Identity Card/QR Code but the Impersonator Fails or Pass the DCQBSP Leading to Impersonation Detection or Attendance Taking	100
Figure 4.12:	Respondent's Views on Mobile Phone User Friendliness	103
Figure 4.13:	Architecture Design of the System.....	105
Figure 4.14:	Generate QR Code with Student Data (Registration number)	112
Figure 4.15:	A Students Registration Interface.....	116

LIST OF ABBREVIATIONS AND ACRONYMS

ARC	Academic Research and Consultancy
DCQBSP	Dynamic Challenging Questions Based On Student Profile
HLIs	Higher Learning Institutions
HLE	Higher Learning Education
IDs	Identifications
OUT	Open University of Tanzania
MNMA	The Mwalimu Nyerere Memorial Academy
NLP	Natural Language Processing
QR Code	Quick Response Code
ICT	Information and Communication Technology
IFM	Institute of Finance Management
DNA	Deoxyribonucleic Acid
ID	Identity
HTML	“Hyper Text Markup Language”
PHP	“Hypertext Preprocessor”
MYSQL	“My Structured Query Language”
CCTV	Closed-Circuit Television
MATLAB	Matrix Laboratory
IP	Internet Protocol
GPS	Global Positioning System
MAC	Media Access Control
APP	Application
IMDIs	Improved Mechanism for Detecting Impersonations.

CHAPTER ONE

INTRODUCTION

1.1 Introduction

Examinations serve as a crucial assessment tool in public higher learning institutions, ensuring that students acquire the required knowledge and skills (MNMA Examinations regulations, 2024). However, academic integrity is increasingly threatened by impersonation, where unauthorized individuals take exams on behalf of registered students (Baijnath and Singh, 2019). This malpractice compromises the credibility of academic qualifications and affects the quality of graduates produced. In Tanzania, public higher learning institutions, including the Mwalimu Nyerere Memorial Academy (MNMA), face significant challenges in detecting and preventing examinations impersonations due to weak authentication mechanisms, inadequate security features in student identification documents, and advancements in forgery techniques (Chow, Serinken and Shlien, 1993).

Current identification methods, such as student ID cards, exam hall tickets, and verification lists, have security vulnerabilities, making it easier for fraudulent individuals to exploit the system. The availability of sophisticated printing technology and online marketplaces for forged identity documents further complicates detection. As a result, there is an urgent need for a more secure and efficient mechanism to authenticate students and prevent impersonation during examinations.

This study aims to develop an improved mechanism for detecting examination impersonation at MNMA by integrating modern authentication technologies. The

research specifically focuses on identifying prominent technologies, designing an enhanced Natural Language Processing (NLP) model, and evaluating its effectiveness. The proposed model incorporates Quick Response (QR) code technology and a dynamic challenging questions generation algorithm and technique to authenticate students in real time.

1.2 Background of the Study

In typical traditional-in-class (physical) learning environment assessment is done through traditional (physical) classrooms, which raise the need to identify the identity of students and their eligibility to take examinations. Impersonations in the other hand is one of the major challenge facing Tanzania public higher learning institutions assessment system where examinations take place in traditional classrooms due to various reasons including poor students' identification schemes; the growth of students' enrollments in public higher learning institutions and high number of students to lecturer ratio which increase the risk of impersonations in these institutions (TCU, VitalStats, 2021) and (Bajinath and Singh, 2019).

A study carried out by Uchenna and Funke (2015) and a study by Ullah, Xiao, and Barker (2019) established the reasons which make higher learning institutions prefer traditional-in-class examinations system including difficulties in identifying students sitting for examinations remotely as they lack face to face interactions and examinations security issues. However, studies presents impersonations as a serious problem which occurs during traditional crass room exams whereby under some circumstances some students invite third parties know as mercenaries to take examinations on their behalf (Bajinath and Singh, 2019); (Garko and Ahmad, 2017)

and (Akinola¹, Abayomi-Alli, and Adeniyi, 2015). The use of third parties (the mercenaries) to sit for examinations on behalf of actual students is always regarded as examination irregularity in all higher learning institutions (Blachnio and Weremko, 2011); (MNMA Examination Regulations and Guidelines, 2024) and (The OUT Prospectus, 2022/2023).

Since examination is formally intended to measure some specific attributes of a learning outcomes including knowledge, skills, aptitude, and proficiency of a student in a particular course, it therefore a service provided by a particular higher learning institution (Bajinath and Singh, 2019); (Bajinath and Singh, 2019); (Rufai and Yekini, 2012) and (Abdullahi Nura and Jiya, 2019). Nevertheless, the 21st century is witnessing an exponential growth in information and communication technology where anyone who wants to authenticate the use of a service including examination is essentially required to have a scheme of identifying the eligibility of an individual who seeks to access that particular service(s), these authentication schemes include identity documents and bio-information (Abdullahi, Nura and Jiya, 2019). Recently, during examinations many public higher learning institutions rely on identity documents such as college identity cards, Examination coupons, examination hall ticket, driving license and national identity card to validate student examination admissibility. Evidence of using the outlined identity documents in Tanzania public higher learning institutions is attached in appendix 1 (a-b) and appendix 2 of this report, subsequently, students hire mercenaries to help them undertake examinations on their behalf especially for courses that are thought to be difficult. Therefore, some students hire mercenaries registered in higher programmes or in a different institution

or even a graduate student who is competent in that particular course. This is impersonations and subsequently an examination irregularity (Lee, Myungjoon 1994); Starovoytova, 2016); (Harding et al, 2006); (Carpenter et al, 2006) and (McCabe, 1997). This happens because identity documents are not enough to verify that student is eligible to seat for a particular examination even when a student may submit forged identity document (Chow, Serinken and Shlien, 1993). Also these students' identity documents does not indicate exactly whether a student is registered for an examination or not.

In some cases, students are asked to come along with other identity documents such as birth certificate or voter's card when they are not given institutional identity cards (see appendix 2). Students' identification schemes of this kind takes much time and efforts, encourage forgeries and provide a room for students to write examination answers that may assist them to pass their examinations. However, in some parts of the world such as Nigeria and Kenya have begun to apply biometric methods such as fingerprints, facial recognition and iris scanning to recognize students (Adigun and Yekini, 2014). In this regards, the use of biometric methods have also proven some critical flaws including spoofing of biometrics and low acceptance rate due to social norms.

Now, flaws existing in current systems for identifying students eligible to take examinations in traditional classrooms strengthen the alarm that public higher learning institutions should see improved impersonations detection mechanism as a highly wanted subject which necessitates serious engagement as part of both their deliberate and operational concern (ICAI and Carter, 2022).

In view of the above, the study on “improved mechanism for detecting traditional-in-class examinations impersonations” was designed and successfully carried out to address the problem. This study was aimed at devising an improved students’ identification scheme that would ensure a correct identification of students who are eligible to take examination or test in a particular course for a particular period of time and thus help in detecting all forms of false identifications. An improved impersonations detection mechanism was owed to incorporate various user authentication methods to improve impersonations detection in Tanzania public higher learning institutions (Masalha and Hirzalah, 2014).

In a nutshell, this study contributes two major things, one, the study proposes an enhanced NLP model that use Questions Generation technique to generate a set of dynamic challenging questions based on student profile which in turn provide an improved impersonations detection mechanism that detects all forms of impersonations that may occur in examinations based on traditional-in-class context using advanced input technologies such as QR code application (scanner) and effective technique that make decisions based on student’s responses for a set of dynamic challenging questions responses and the study stimulates further studies in the area of integrating artificial intelligence and Education security.

1.3 Statement of the Research Problem

Students’ identity cards, Examination Hall tickets and examination coupons are major documents that are used as a means of checking the authenticity, validity and eligibility of students to take traditional-in-class examinations in most public higher

learning institutions (Abdullahi, Nura and Jiya, 2019); (MNMA Examination Regulations and guidelines, 2024); (OUT Prospectus, 2022/2023); (IFM Prospectus, 2022/2023) and (Patrick, McOyowo and Okoyo, 2015). These students' identification schemes have Security vulnerabilities that can be exploited by individuals seeking to impersonate others. These vulnerabilities include weak authentication features, lack of encryption, or insufficient anti-counterfeiting measures which make impersonations detection in most public higher learning institutions more challenging. Also there is an advanced access to printing technology which make it easy for individuals to access high-quality printing and graphic design tools, making it possible to create convincing fake identity cards. In addition, in Online Market places forged identity cards can be purchased. These online sites often claim to replicate official Identity cards with high accuracy. In this regard, an improved mechanism (a model) for protecting identification documents (ID) against forgery, tampering and detecting fake identity documents that encourage impersonations is of paramount importance.

1.4 Research Objectives

This section states the objectives of this study including both general objective and specific objectives.

1.4.1 General Research Objective

The study seeks to achieve its general objective of developing Improved Mechanism for Detecting Examinations Impersonations in Public Higher Learning Institutions; Case of The Mwalimu Nyerere Memorial Academy (MNMA).

1.4.2 Specific Research Objectives

The general objectives stated in subsection 1.4.1 have been achieved through meeting the following specific objectives:

- i. Identifying prominent technologies suitable for detecting impersonations during traditional-in-class examinations.
- ii. Developing an enhanced natural language processing (NLP) model which detects impersonations in the context of traditional-in-class examinations.
- iii. Evaluating the efficiency of the developed NLP model which detects impersonations in the context of traditional-in-class examinations.

1.5 Research Questions

This section presents research questions that will be addressed in achieving the aforementioned objectives.

1.5.1 Specific Research Questions

These research questions are in line with specific objectives stated in subsection 1.4.2 and they were trying to stimulate the acquisition of information that facilitated the achievement of those specific research objectives. Following are research questions that this study expected to answer:

- i. What are the prominent technologies suitable for detecting impersonations during traditional-in-class examinations?

- ii. How to develop an enhanced NLP model which detects impersonations in the context of traditional-in-class examinations?
- iii. What aspects to consider when evaluating efficiency of the enhanced NLP model which detects impersonations in the context of traditional-in-class examinations?

1.6 Relevance of the Research

Public Higher learning institutions in Tanzania and beyond are challenged to address the issue of impersonations during traditional-in-class examinations proactively, responsively and justly. The consequences of failing to do so are underlined and examples are given of what can and has already been tried and tested to lessen the menace (Bajinath and Singh, 2019). Impersonations detection models necessitates the need to conduct a case study that can produce not only an improved mechanism for detecting impersonations in traditional-in-class examinations in Public higher learning institutions proactively but also to add knowledge to the already known schemes and models for detecting impersonations, ultimately helps higher learning institutions to deal with impersonations with a global lens which take the advantage of the advanced computing and information technology in the area of artificial intelligence (Madara and Namango, 2016) and (Diedenhofen and Musch, 2016).

The rest of the dissertation report is organized into chapters, chapter two provides a critical review of the literatures and theory related to this study, chapter three describes a research methodology which guided this study, chapter four presents findings and discussion while chapter five presents conclusion and recommendations for future work.

CHAPTER TWO

LITERATURE REVIEW

2.1 Overview

This chapter explores various studies connected to impersonations and impersonations detection mechanisms that enable public higher learning institutions to deal with impersonations in traditional-in-class examinations. The review provides empirical evidence on the existence of impersonations fraud in examinations systems in many higher learning institutions worldwide and the outcomes posed by this pandemic. Furthermore, the review provides a practical foundation of what has been done to uncover impersonations and provides a real picture and the need of developing an improved mechanism for detecting traditional-in-class impersonations that can be adopted by all public higher learning institutions in Tanzania.

2.2 Conceptual Definitions

This section provides definitions of various concepts presented in this documents so as to facilitate the understanding of any reader of this document any time he or she come across these terms and concepts.

An impersonation as defined by Cambridge Dictionary refers to the act of trying to deceive or mislead others by pretending that you another person. A student requests a mercenary to seat for examination on his/her behalf (Lee and Myungjoon, 1994) and (Ullah, Xiao, and Barker, 2019).

A machine learning model is a program that can find patterns or judge a phenomenon from a previously unseen dataset. For example, in a natural language

processing, machine learning models can parse and correctly recognize the intent behind previously unheard sentence or combinations of words (Emily, 2019).

NLP models operate by identifying connections between the elements of language, such as the letters, words, and sentences within a text dataset. NLP frameworks employ different techniques for data preprocessing, feature extraction, and modeling (deeplearning.ai).

Higher learning or higher education implies any type of education given in postsecondary institutions of learning which leads to various awards such as Degree, Diploma or certificate of higher studies (Justus et al, 2022); (Mukerji and Tripathi, 2013). Higher learning institutions include not only universities and colleges but also various professional schools that provide preparations in such fields as Computer Science, Philosophy, Chemistry, Mechanical Engineering, Petroleum Chemistry, Dentistry, Fine art, Education, Clinical Medicine, Mining, Library, Tourism, Mathematics and Architecture planning (The Tanzania Commission for Universities: VitalStats on University education in Tanzania, 2022). Higher learning institutions in Tanzania include The Open University of Tanzania, and The Mwalimu Nyerere Memorial Academy.

Also Detection as defined in oxford dictionary is the act or practice of ascertaining the presence of something unknown. A mechanism is generally defined as any object or system that has a working part or parts. Most often the term suggests tools, instruments, and machines (worldpress.com).

Furthermore, *fake identities* implies identity which conglomerate forged material with genuine identification card facts. For example, combining a real social security number along with a fake address and other synthetic data points (fraud magazine.com).

Traditional-in-class examinations: This is where trainers take complete control of the examination process by designing questions, grading, setting up examinations and physically invigilating students to conduct these examinations in examination halls. (Shen, Cheng, Bieber and Hiltz, 2004).

2.3 Critical Review of a Supporting Theory

Impersonations in a traditional-in-class examination environment is currently proliferating and it is among of the fastest growing academic dishonest in Tanzania and beyond (Clarke, 1994); (Modal, 2022) and (de Aquino and Yambi, 2022). Impersonations is caused by existing identity verification schemes which contains flaws that lay down the foundation of impersonations fraud. The advance of impersonations in many public higher learning institutions appears to be symmetrical, reflecting the fact that the examination eligibility check system has no effective filtering mechanism that would ensure that only correct candidates enters the examination venues. To commit impersonations two parties need to arrange the mechanism by which a mercenary will deceive the invigilator into believing that he or she is a correct (eligible) examination candidate while it is not. To achieve this the mercenary will imitate all information necessary to identify a student as being eligible to sit for examination.

Many strategies to fight against traditional-in-class examinations impersonations in public higher learning institutions have been suggested focusing on making it more difficult for mercenaries to obtain access to such traditional examination venues. As it is illuminated in section 2.6, these strategies are deemed to failure because they depend upon methods or techniques that are subjected to human manipulations. This implies that, reliable techniques should be resistant to any form of manipulation for them to ensure that only correct candidates enter and sit for examinations.

This study proposes an improved mechanism (solution) to impersonations detection in traditional-classroom examinations. The solution conceptualizes impersonations problem as a failure in human identification. The problem is not that impersonators (both the student and the mercenary) have right and ability to penetrate the identification door, rather existing identification schemes often lack both the means and incentives to correctly identify the student who is eligible to enter the examination venue and sit for examinations. The proposed solution set forward addresses all flaws in the existing students' identification schemes by designing an improved mechanism that helps higher learning institutions authorities to correctly identify students eligible to seat for examinations and detect all impersonations.

It is with due understanding that to design an improved mechanism for detecting impersonations which solves impersonations problem in public higher learning institutions' traditional-in-class examinations systems required a deep theoretical background on the process of human identification and the role that misidentifications play in committing impersonations.

For that reason, sections 2.4 illuminate a positive theory of human identification which is reliable in specifying methods and variables that are relevant for human identification today.

2.4 The Theory of Human Identification

In the article of Human Identification in Information Systems: Management Challenges and Public Policy Issues, the author defines human identification as the process of establishing the identity or recognizing a thing or establishing as being a particular person (Clarke, 1994). The author states that for the ground of record systems, these definitions are rather abstract and unhelpful. Also information technology dictionaries have less or no assistance such as the Penguin Dictionary of Computers does not give any definition regarding human identification and that both the definition for file identification and identifier depend on the meaning of the word identity which is not defined.

However in the domain of information systems, the goal of identification is very concrete as it is used to associate data stream with a person. Therefore; this review describes human identification as the link of data with a particular human being (Clarke, 1994). The human identification theory stands in the positive view that human identification is appropriate to data that are stored in a structured, physical and manageable form as in a corporate databases and documentary filing schemes; but also it applies to data stored in a less formal system, as in private notes; and in intangible form, as in ballads and human memory (Clarke, 1994). Clarke (1994) suggests that the principle behind human identification were social rather than

economic. A person had to be identified himself or herself with a group. Certainly, group-membership such as one of us or one of them was possibly a significant matter than individual identity throughout pre-historic times and most of the historic era. Context were used to identify Relatives, friends and acquaintances where physical appearance, voice characteristics, knowledge of private information, location and espoused name all play a part. Further description in the theory proposes that these features are reliable when they stand individually, they only apply when peoples involved are in close domain, and they depend upon human memory, with all its emotions. However, these features are adequate for most social purposes.

The importance of human identification arose due to the need for parties to know with whom they were dealing. The situation became normal for parties to supply their information among themselves which were appropriate to nature of transaction. This were an overt identifier for instance, the property the person owned such as car. Equally, some pieces of information might together identify a person for instance “Meet me at college in the boardroom, I will be seating around the corner” . Again human identification was important to provide a gesture of goodwill, to develop mutual confidence, and to reduce the scope for dishonesty; to facilitate communications and to enable person link transactions and information with the other person. To save this purpose human identification must have an adequate basis. The theory suggests that several evidence could be used for identification depending on either intrinsic or physical features of the human. In real sense a human is accepted as being a human to whom a record relates because he or she represent he(r)self as being that human , he or she know things that in the normal course of

events only that human would be expected to know, they do things such as mentioning coursework score that would only be in the interests of that person to do, or they possess material or document or token which it is reasonable to expect that human to possess. In practice it is common to apply various techniques in integration. Studies that compliment human identification theory of many ages and cultures have taken opportunity of the scope for mistaken identity, such as Shakespeare and Gilbert and Sullivan providing manifold examples. All identification schemes have flaws and therefore, most of transactions involve risk and cost money. The primary focus of this theoretical analysis is to build a foundation where public higher learning institutions can utilize rational process to implement schemes which balance the costs, the benefits and the risks involved.

2.4.1 Bases for Formal Identification

The Clarke's theory (1994) identified several mechanisms for making human identifications. These include: appearance, social behavior (interactions), names, codes, knowledge (what the person knows), tokens (what the person has), bio-dynamics (what the person does), natural physiography (what the person is) and imposed physical characteristics (what the person is now). The description of the bases for formal identification mechanism is given below.

2.4.1.1 Names as a base of identification

As a basis for identification, names lack constancy and reliability;

- i. have different sequences between institutions for example in one institution family name may appear first;

- ii. some names have additional components for example a name of religious rather than identificatory significance;
- iii. some names may be incomplete for example there may be no family name;
- iv. names may be assigned in unfamiliar ways for example the surname may come from the matriarchal rather than patriarchal line, or by leap-frogging generations;
- v. A further challenge arises from mis-spellings and variations;
- vi. change in ways or at times foreign to local tradition for example at puberty and
- vii. Some names may be variable depending on the context for example by omitting the religious component.

Studies that support this theory recommend that in order to handle these doubts, further data should be used as additional elements of the identification, or as confirmatory data. Such data include but not limited to date of birth and personal address. However date of birth suffers from being, for some people, particularly sensitive and address is also sensitive for some people, and is volatile. In a nutshell using names for human identification is a bit challenging and pose a doubt on building an organizational identification system on names.

2.4.1.2 Codes

To solve the challenges of names for identification some organizations create coding schemes based on a set of strings. Codes enable organizations to control issuing of

codes and maintain uniqueness of the codes. Individuals are required to remember those codes assigned to them by the organization. Sometime individuals are issued with token bearing codes, and requested to bring those tokens with them when they intend to perform some transaction that requires identification. Codes should be human-readable, machine-readable, or both. For example a QR code is a current popular method of keeping codes on product and packages in such a way that devices can read the QR codes and card borne magnetic stripes and memory-chips can also contain identification codes.

2.4.1.3 Knowledge-Based Identification

Human can be identified by proving that they are possession of information which only that person would be expected to know. Examples of such information include family names, date of birth, school information, mother's and grandmothers' middle names, coursework results, place of birth, address, marital status, religion, and occupation. However some human can fail to know such information or forget them at all but this approach to human identification is a reliable means of identifying an individual and can be implemented in organizational information systems. Many scholars implemented system models that utilize the concept of knowledge analysis to generate questions that are used to verify the identity of users. These systems typically rely on pre-set questions and answers to verify the identity of users commonly known as static questions.

Generating static questions based on a system user profile involves a combination of techniques from various fields such as information retrieval, natural language

processing (NLP), and machine learning. More specifically these systems use algorithms and techniques including Rule-Based Systems (algorithm) which use techniques such as Decision Trees and Expert Systems; Template-Based Generation algorithm which applies techniques such as Slot Filling and Parameterized Templates; Collaborative Filtering algorithms which are typically used in recommendation systems, these algorithms use techniques such as User-Based Collaborative Filtering and Item-Based Collaborative Filtering.

Content-Based Filtering which uses the attributes of the user profile to directly match and generate relevant questions, techniques used include TF-IDF (Term Frequency-Inverse Document Frequency and Word Embedding like word2Vec or BERT to understand the semantic meaning of user profile attributes and generate contextually relevant questions. Lastly but not least, Natural Language Processing (NLP) algorithm is used to generate static question, this algorithm applies techniques such as Named Entity Recognition (NER) which identifies entities such as names, dates, and locations in the user profile to generate specific questions as well as Sentence Generation Models like GPT-3 or GPT-4 to generate human-like questions based on the context provided by the user profile. Other algorithms include Hybrid Approaches (Hybrid Filtering, and Ensemble Methods), Machine Learning Models (Classification, Neural Networks and Clustering algorithms) and Personalization Algorithms (Reinforcement Learning and Contextual Bandits).

Moreover, systems that use static questions algorithms for user verification are common in various sectors, including banking, healthcare, and online services.

Below are some sample systems and descriptions of how they implement static question-based identification.

2.4.1.3.1 Banking

Numerous banks such as the CRDB and the Barclays Banks Mobile Banking applications use static security questions as a part of their multi-factor authentication process. During the account setup, users select or create answers to specific questions. These questions include but not limited to "What is your favorite food?"; "What is your next of keen last name?" and "What is you secondary school name?" The implementation of these systems involve phases such as Implementation: the Enrollment phase where users select questions from a predefined list and provide answers, the second phase involve authentication when users access their account from a new device or location, they are prompted to answer one or more of these questions and the last phase in verification where the system checks the provided answers against the stored responses.

2.4.1.3.2 Healthcare Systems

Healthcare Systems such as a Patient Portal Access are another systems which implements static questions models to authenticate patients before granting access to sensitive health information through patient portals. Like in the banking systems, the implementation of Healthcare Systems also involve enrollment, authentication and verification where the system compares the answers with those on record.

2.4.1.3.3 Online Services and E-commerce

In addition, most Online Services and E-commerce platforms such as Amazon, e Bay

and email providers, use static questions for account recovery and additional verification. The implementation of these systems equally applies similar rule of enrollment, authentication and verification to accomplish user identification and impersonations detection.

2.4.1.3.4 Government Services

Also, Government tax agencies sometimes use static security questions to verify taxpayers' identities before granting access to online tax filing systems. The implementation of these systems follow an enrollment, authentication and verification phases as stated in the previous sections.

2.4.1.3.5 Education Systems

Moreover, education institutions often use static questions to secure student portals, where students can access their academic records, course materials, and personal information.

2.4.1.3.6 Summary

While static questions can provide an additional layer of security, they are generally considered less secure compared to dynamic challenging questions or multi-factor authentication methods due to their susceptibility to social engineering and guessability (AlHusain and Alkhalifah, 2022). The reasons for their poor security include factors like complexity and uniqueness which encourage users to select complex, unique answers that are difficult to guess or find through social media, limit attempts by implementing a mechanism that limit the number of attempts to

answer security questions to prevent brute-force attacks and regular updates which allow users to update their security questions and answers periodically as well as an encryption issue which requires to ensure that both the questions and answers are stored securely using encryption.

2.4.1.4 Token-Based Identification

A token refer to something that an individual hold or possess in a document form as an evidence. Such documents include birth and marriage certificates, passport, driver's license, employer-issued building security card, credit card, club membership card, statutory declaration, affidavit, or letter of introduction. Studies show that token based identification scheme is applicable when environment is under tight control. However these tokens can be forged leading to impersonations (Tanvi, Sonal and Kumar, 2011).

2.4.1.5 Biometrics

Biometrics refer to all forms of identification which are based on physical and physiological body features which are difficult to alienate. This approach is believed to provide maximum confidence that the identification is accurate. Biometric approach involve metrics of some kind rather than relying only on informal methods. Examples of biometric techniques include physical Appearance, Social behavior, Bio-dynamics, Natural physiography and Imposed physical characteristics. However biometric method is also contained with challenges such as natural and artificial changing of Biometric features, some biometric feature such as DNA test are

protected by laws and biometric features can be spoofed leading to incorrect identification.

Generally human identification theory facilitates the development of a reliable impersonations detection mechanism that integrate two or more human identification schemes to mitigate the challenges existing in current human identification schemes in many public higher learning institutions.

2.5 Empirical Analysis of Relevant Studies

Researchers and Education Scholars have presented various form of examination cheating in higher learning institutions including gaining unlawful assistance or information; giving unlawful assistance or information; committing plagiarism from written, internet sources such as when a student turns in an exceptional report that the supervisor doubts its legitimacy; falsifying the facts; posing bribes; and Impersonations (Madara and Namango, 2016); (Forgas, Lancaster, Sastre, Negre, 2021); (Noorbehbahani, Mohammadi & Aminazadeh, 2022) and (Anderson, 1981). Impersonations in the other hand is a serious examinations cheating behavior and is against the goal of higher education which emphasize on quality, competence and individual development (Modal, 2022); (de Aquino and Yambi, 2022) and (TCU, VitalStats, 2021). Yet there is a lot of studies published in various journals and repositories, that when read together illuminate on the truth that higher learning institutions globally experience impersonations that compromise with education quality yet existing schemes for detecting impersonations are associated with numerous limitations (Bajjnath and Singh, 2019); (Bait Garko and Ahmad, 2017) and (Akinola¹, Abayomi-Alli, and Adeniyi, 2015). This study presents

impersonations as a serious examination fraud in public higher learning institutions based in Tanzania context that requires serious attention and remedial.

2.5.1 Current Techniques for Detecting Impersonations during Traditional-In-Class Examinations

The study carried out by Akaranga and Ogong (2013) in Kenya insists the need to enforcing strategies against the menace in academic institutions, in that regard, a severe combined moral method to eradicate impersonations from their academic institutions were recommended. Njoku and Njoku (2016) conducted a study titled “Curbing Examination Malpractice in Secondary Schools in Nigeria through Moral Education”, in this study authors proposed the teaching of ethical education as an effective means of cutting the menace and the idea was well supported by uma, Nnandi, and Nche (2014). However teaching moral education has proven that not all people believes in religious or cultural values hence leaving impersonations as a paradox to many.

Also this review went through numerous studies that aimed at preventing impersonations by using examination eligibility verification and attendance system which relies on a quick response (QR) code that are embedded in students identification cards and validated by smartphone (for scanning the QR code generated). Examples of such studies include the study conducted by Abdullahi, Nura, and Jiya in 2019 and another study conducted by Falguni, Utkarsha, and Madhuri in 2015. Abdullahi, Nura, and Jiya (2019) proposed a web based examination eligibility verification system which use QR code technology. The

examination eligibility verification system was effective and reliable in verifying student identity over the existed student identification scheme. The examination eligibility verification system involved two parties namely the invigilator and student. Also each student registered by the institution must have identity card. On the other side, a web camera is attached to personal computer system. Thus, QR code images are embedded in an identity card, which can be scanned by an invigilator using the web camera to identify the validity of a student. This implies that, a student's ID card must be scanned by an invigilator to check his or her examination eligibility.

The system display eligibility status whenever it finds that a student is registered. In the contrast the system display a not eligible status. Students ID card is scanned twice to ensure student login and student logout. To achieve system objective, the examination eligibility verification system was divided into two parts, the enrolment part and verification part. The enrollment section facilitates students in registering their credentials, while the verification section allows invigilators to confirm student examination eligibility. The architecture of the examination eligibility verification system followed the MVC (Model, View, and Controller) model, which offers a structured approach. In this model, the interface with the system database is handled by the model, application logic is managed by the controller, and user interaction is facilitated by the view.

The front end of the examination eligibility verification system was developed using JavaScript, Cascading Style Sheets, and HTML5 within Microsoft Visual Studio

Code, while the server side was implemented using PHP and MySQL database management system. Chrome web browsers was used to access the system (more description of the implementation is presented in the research paper). Findings from this study show that time taken to accomplish student verification task was four seconds. This implies that the system could verify 1000 students within an average of 1 hour when operated by only one invigilator but if two or more invigilators are involved in the verification process then less time could be used to verify 1000 students (Abdullahi, Nura and Jiya, 2019). With regard to QR code technology, numerous studies recognize the utilization of student identification cards equipped with QR codes as a means of authenticating and identifying students eligible to take examinations.

However, when these identification cards are handled manually they become infeasible due to high number of candidates compared to available examinations invigilators. Also, since human cannot read QR codes, it is possible for attackers to change it to the extent of accessing protected resource without being detected. QR code can trigger user's device and add unnecessary information to the database. This can eventually compromise with the intended purpose of the system. Therefore more harsh mechanism should be enforced to limit access to protected resources merely by QR code (Kaspersky, 2023). It is suggested that supplementing a QR code system with another level of identification is important for system robustness. Therefore, the Abdullahi, Nura and Jiya (2019) impersonations detection system could be modified in terms of functionalities and scope so as to add more security and usability.

The system could not end up displaying eligible or not eligible statuses but could have supplied much more information required for effective verification purposes. Another study which implemented QR code technology as a means of screening ineligible students include; a study by Ayeleso, Adekiigbe, Onyeka, and Oladele (2017): “an offline identity card authentication system using QR code and Smartphone”. Nevertheless, other studies suggested different options for curbing impersonations for example a study conducted by Onuka and Durowoju (2011) recommends various strategies for combating examination malpractice which should include but not limited to applying appropriate sanction on the culprits, corporate fight against examination malpractice, building large examination halls, stakeholders should jointly educate responsible parties on the appropriate measures that can help to fight examination fraud, constant comprehensive inspection of a school system and other related means, this study encourage examination bodies in Africa to adopt the KTE-IMS software for computerized assessment of candidates owned by the Kenya examination board.

The KTE-IMS software gives a mechanism for computerized objective questions such as Multiple choice questions and True or false questions, and it guarantees an automatic generation of students’ scores after they have submitted their examinations. However the KTE-IMS software helps to fight examination fraud in computerized assessment of candidates, it does not provide a detailed implementation of the KTE-IMS software apart from recommending it as part of strategy for “Curtailling Examination Fraud for Improved Quality Assurance in the African Examination System”. Also this study is too general to conclude

impersonations fraud in Tanzania higher learning institutions, as sample size used included only 20 secondary school teachers and 400 secondary school students and the nature of examination malpractice observed were too general to be associated with impersonations.

Adigun and Yekini (2012) placed a major concern on impersonations and the technique for detecting impersonations in Yaba College of Technology in Nigeria. The study shows that several steps have been taken to combat impersonations in Nigeria but impersonations have remained at the pick in the country. The study identified several techniques for detecting impersonations including the use of Identity Cards to authenticate students; the application of many invigilators to identify false candidates; the distribution of sitting plan number that decides the room where the candidate will write examination and the prerequisite to sign in and out on the attendance sheets. Adigun and Yekini insist that genuine verification of the candidate's identity before entering the examination venue must be a major concern. Finally Adigun and Yekini proposed a Biometric Model (fingerprint) which solve the problem existing in current techniques used for identifying students and detecting impersonators at the college.

The model identifies every student at the entrance point of the examination venue. The model was found to be efficient compared to manual student's verification system. Nevertheless, the model was found to have several challenges such a spoofing of biometrics that is the use of forged biometric object such as plastic fingers in accessing a secured system, this can be achieved by using Artificial fingers

which can be created from the casts using gelatin, commonly used for confectionary, where the resultant casts are termed “gummy fingers”. The problem of artificial fingers can be solved by live detection where the biometric being captured is determined to see if it is a concrete measurement from the approved, live person who is existing at the time of capture or other methods as may be found effective. Also biometric template has security issue. When it is compromised the user drops his or her identity for life.

The recommendation is that more techniques must be applied in developing a more robust liveness detection mechanisms that removes the risk of spoofing and pledge a correct identification of student. In regard to biometric implementations several studies have been evolved since then even using other biometric traits such as Face, iris and sound. Such studies include a study by Iwasokun, Omomule, and Olufemi Akinyede (2018) and a study by Onaolamipo (2014) which implemented a “Computerized Biometric Control Examination Screening and Attendance Monitoring System with Fees Management. However, these models suffer several times as they had low user acceptance due to cultural and social challenges as well as being susceptible to human manipulation. Moreover, Garko and Ahmad (2017) designed and modeled a Student Verification System in an Examination in Nigeria using Biometric Fingerprint Technology. Akinola, Alli and Adeniyi (2015) also implemented a fingerprint system for verifying students.

In addition, Eziechina, Ugboaja and Esiagu (2017); Hoque, Ahmed, Chittagong, Uddin, and Faisal (nd) equally Proposed a mechanism which requires educational

institutions to store a database using Parallax Data Acquisition tool (PLX-DAQ) that incorporates bio-metric information of all students. The system authenticates students during examinations and monitor examination progress by using fingerprint sensor module and 360-degree Closed-Circuit Television (CCTV) cameras as well as ultra-high sensitive microphones and speakers respectively. These studies however were aimed at replacing complex traditional-in-class examination invigilation system by reducing costs and increasing examination security.

Another Study conducted by Binu, Bhuvana, Karthika and Kayalvizhi (nd) suggests that impersonations in examinations hall can be reduced by verifying students using bi-modal features of the candidate. The study proposed a system which consists of bi-modal scanner connected to Raspberry Pi and data stored in MATLAB database. However the system requires high installation cost resulting to low acceptance rate due to cost, cultural and social phenomena, as well as accessibility issues which limits the application of this solution in many parts of the world. Also biometric system is not capable of capturing the original fingerprint images from the scanner; rather, it can only accept the fingerprint templates from a server.

Moreover, Eziechina, Ugboaja and Esiagu (2017) study suggests an effective examination invigilation which can help to prevent several examination malpractices including impersonations. In their view a closed-circuit television (CCTV) surveillance system can be used in Nigeria to save the same purpose. However this system cannot be used for detecting and identifying impersonations fraud that occurs due to poor students' identifications. Also the system is expensive since it depends

on the quality of the camera, monitor and recorder. On the other hand, other studies on impersonations detection suggested the use of barcode technology as a suitable mechanism to replacing traditional techniques of identifying students and detecting impersonations. These studies include but not limited to Elaskariab, Imrana, Elaskric and Almasoudi (2021): “Using Barcode to Track Students Attendance and Assets in Higher Education Institutions” and a study by Saheed, Adedeji, and deniji (2016): “Attendance Management System Using Barcode Identification on Students’ Identity Cards”. These studies suggest that barcode based systems solve the problem of impersonations existing in traditional-in-class context. Studies show that barcode solutions are easy to implement, inexpensive in terms of cost, and effective in terms of reliability and efficiency. A concern, however, might be in the area of maintenance (Saheed, Adedeji, and deniji, 2016). Another challenge associated with a barcode technology is its low capacity for storing information. Due to these reasons a barcode technology is smoothly being replaced by a QR code technology (Abdullahi, Nura, and Jiya, 2019).

In a nutshell, the review of some available literatures adds to the understanding that impersonations in higher education is considerably greater than the strategies that are being used to deal with impersonations in Tanzania public higher learning institutions and the world at large. Given the conducted studies on impersonations detection mechanisms represent the absence of a holistic mechanism for dealing with impersonations detection not only in Tanzania Public Higher Learning Institutions but also beyond Tanzania boundaries. Therefore, a study towards the development of an improved mechanism for detecting impersonations especially in Tanzania Public

higher learning institutions is of paramount importance (Bajinath and Singh, 2019); (Diedenhofen and Musch, 2016); (Bajinath and Singh, 2019); (Madara and Namango, 2016); (Diedenhofen and Musch, 2016) and (Madara and Namango, 2016).

2.5.2 Impersonations Detection Mechanisms Related to this Study

Several researches have been carried out to provide mechanisms for detecting impersonations especially in traditional-in-class examinations. One of them includes a student authentication framework for online examinations outside of school by Urosevic (2019). This study aimed at finding out how institutions can correctly identify eligible students for examinations that are done online. In this study various identification techniques were described such as the use of pin code, facial recognition, voice, keystroke, fingerprint, profile-based authentication as well as hand geometry based recognition.

Findings from this study reveals that biometrics, security, data protection as well as two-layer authentication should be emphasized in impersonations detection or identity check framework for online examinations (Mening, 2017); (Ramu et al., 2013) and (Ashibani and Mahmoud, 2017). Nevertheless, some studies reveal a lots of weaknesses and security vulnerability associated with these approaches (Agashe and Nimbhorkar, 2015). For example, knowledge-based authentication approach such as the use of pin code and password necessitate owners to recall authentication credentials, which may be vulnerable to attacks. For the Object-based approaches a user is obliged to have tokens that are likely to be loss or stilled. Also this approach

is impractical for users to constantly have tokens, especially those users who have many identification tokens (Li, Wang and Sun, 2017).

Therefore, a constant login verification scheme such as behavioral biometrics (keystroke dynamics, mouse dynamics, signature, Gait and voice), physiological biometrics (face, finger, iris, retina and ear) and multimodal biometrics (a combination of two or more biometrics features) come to resolve these problems (Ayeswarya and Norman, 2019). The mechanism is as shown in Figure 2.1

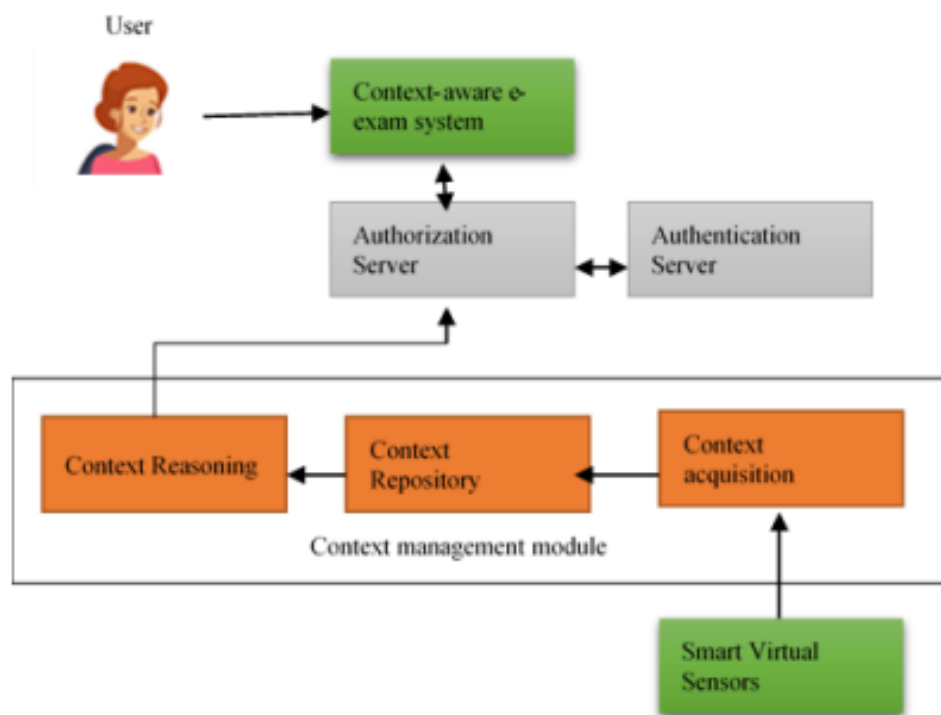


Figure 2.1: Context-Aware E-Examination Architecture Framework

Source; Murugesan and Gangadharan, 2012.

As shown in Figure 2.1, the contextual information will be picked up by virtual sensors by means of suitable virtual sensor technology for context information

acquisition. These data will be processed and made accessible in a machine-processable format to the authorization server. Contextual Information Context type Characteristics include User context GPS Time zone, Connection type Log profile, Device context, Operating system, Browser, Access point, MAC address, Installed App, Device features, Network context IP address Connection type, Ping Environmental context, Lighting and Noise Loudness.

Also Anandhavalli, Natchiyar, Deepshika, and Priyadharshini (2020) developed a mechanism for an automated fraud detection to detect the impersonations of candidates and possession of electronic gadgets by the candidates in an examination hall. The impersonations of the candidates and the presence of electronic gadgets have been detected by image processing techniques for detection and recognition and machine learning algorithms (Random Forest algorithm and Histogram of Oriented Gradients (HoG) algorithm) for the classification. These algorithms have been selected for the high accuracy that they provide in detecting and recognizing datasets. They require a smaller number of training datasets when compared to other models to perform efficiently.

The aim of developing this mechanism was to reduce the human effort in invigilation of an examination hall and provide a highly efficient candidate monitoring system. The proposed automated fraud detection mechanism in examination halls based on machine learning is thus a work in progress and a huge number of features can be added to make it more user friendly and efficient. Some of the features in development include adding an alarm system and candidate emotion detector system to detect the level of difficulty of the examination. The system will serve as a cost

and performance efficient solution to monitor the behavior of candidates in an examination hall.

2.6 Research Gap

From the theoretical review and empirical analysis described in sub-section 2.4 and subsections 2.5, it has been clear that impersonations detection in traditional-in-class examinations is a global challenge that hampers the quality of graduates and education assessment system at large. Despite the fact that several scholars have conducted studies, and presented impersonations detection schemes and the principle behind impersonations fraud in traditional-in-class examinations neither public higher learning institutions nor governments has created a robust and holistic mechanism for addressing traditional-in-class impersonations. Most of current mechanisms for detecting impersonations for example the use of identity documents are subjected to challenges such as forgery, lose and theft. Spoofing of biometrics and cultural reluctance towards the use of biometrics as a base for human identification pose a challenge on the use of biometric identification schemes.

This implies that most of the existing impersonations detection strategies are less user friendly, less robust and holistic. Yet studies on impersonations detection models especially based in Tanzanian public higher learning institutions context are very limited. In this regard a comprehensive study towards the development of the enhance NLP model for detecting impersonations in traditional-in-class examinations is of paramount importance. The model owed should be able to check the eligibility of students to take examination and detect impersonations fraud before or during

examinations without compromising the integrity of student information. In addition, the impersonation detection model should ease the task of examination irregularity syndicate, reduce time and efforts required to deal with impersonations cases, facilitate communication between relevant parties affected by impersonations and enables invigilators to take students' attendance automatically during identification process. This saves examinations invigilators' time and encourage students who plan to engage in impersonations to prepare well for all examinations.

2.7 Focus of the Research

This study focuses mainly on developing the NLP model that is cable of filtering out all ineligible candidates and allow only candidates who are eligible to sit for examinations. Particularly, the study aims at using relevant NLP technique particularly a QG and QR code techniques that can generating dynamic challenging questions based on student profile. Given this implementation, impersonations can be accurately detected and reported to relevant institution authorities. This is to create a two level impersonations detection mechanism which can be applied in traditional-in-class examinations of the public higher learning institutions. The proposed improved mechanism or simply the NLP model automatically generates dynamic challenging questions based on student profile that a student must answer before being allowed to access an examination venue.

2.8 A conceptual framework of an Improved Mechanism for Detecting Traditional-in-Class Examinations Impersonations in Tanzania Public Higher Learning Institutions

The diagram in Figure 2.2 describes a conceptual framework of an improved mechanism for detecting traditional-in-class examinations impersonations in Tanzania public higher learning institutions.

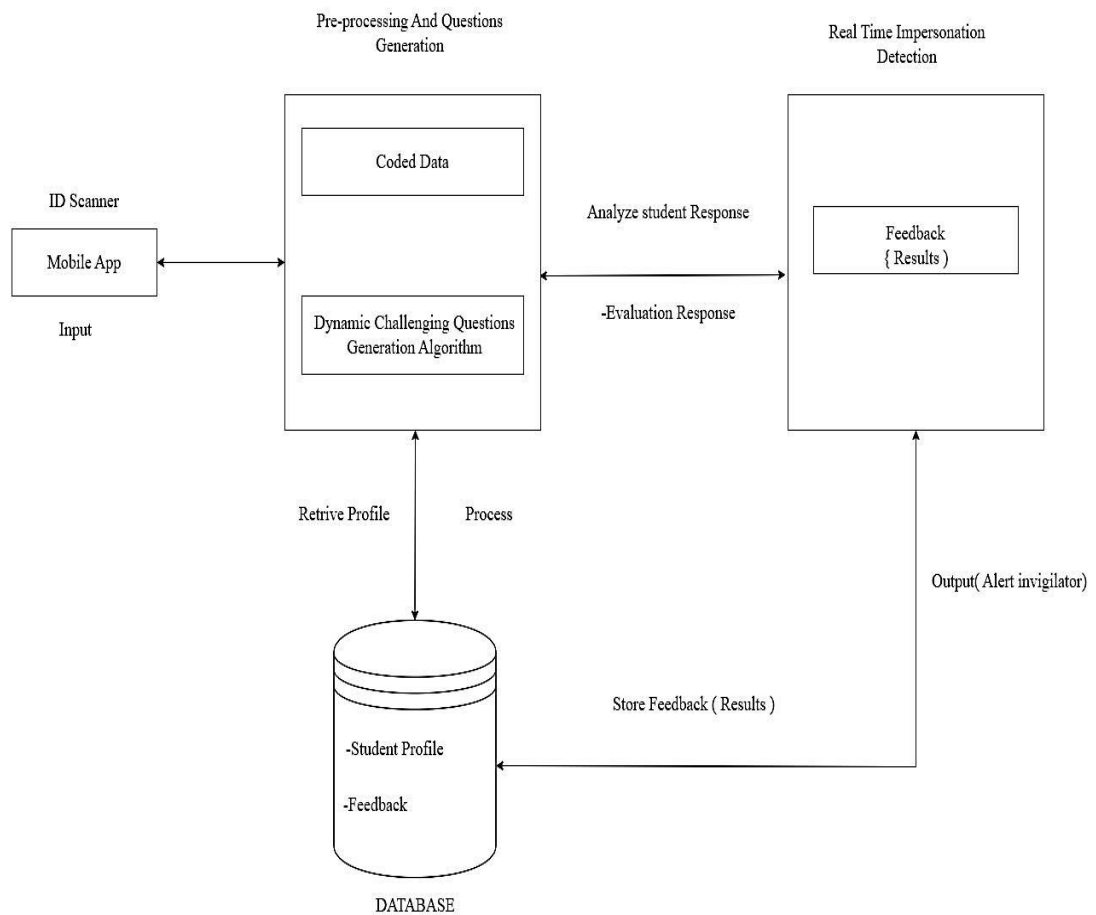


Figure 2.2: A conceptual framework of an improved mechanism for detecting Traditional-in-class Examinations Impersonations in Tanzania Public higher Learning Institutions

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Overview

Kothari (2014) defines research methodology as way of solving a research problem systematically. It involves studying various steps embraced by a researcher in studying a problem along with the logic behind them. Kothari insists the need for the researcher to know not only the research methods or techniques but also the methodology. For example, knowing only how to create certain indices or tests, computing means, modes and median, the standard deviation, chi-square, applying specific research techniques is not enough until he or she understand which of these techniques are pertinent and which are not, and what would they mean and designate and why. In addition researchers should comprehend the assumptions underlying several techniques and they need to know the conditions by which they can decide that certain techniques and procedures will be appropriate to definite problem and others will not. This implies that designing a methodology for a specific problem is a crucial step for any research task.

In view of the above, this chapter describes a research methodology and strategy designed for conducting this study, sample frame and sample size, sampling design methods, data collection methods, data processing methods and data analysis methods are enlightened as well. Finally this chapter provides the expected research output.

3.2 Research Strategy

Based on the selected research theme and based on the fact that Qualitative research

method is always used by information systems researchers (Orlikowski and Baroudi, 1991) and (Alavi and Carlson, 1992). Using case study research design method helps to investigate a contemporary phenomenon in the context of its real life especially when there is no clear demarcation between phenomenon and its context. Studies show that when the “how and why” enquiries exist, a case study should be the most relevant research strategy (Wedawatta, Ingirige and Amaratunga, 2011). The case study is most usable when the phenomenon dissociated from its context (Kobziev and Al Kilani, 2016). Case study applies qualitative methods and it is most applicable in information system researches. Also a case study is very helpful when investigating a contemporary phenomenon which is not clear.

A study conducted by Kobziev and Kilani (2016) identify three reason that lead to the selection of case study strategy when conducting study in the field of information system (IS): First, a case study helps to study information system in its natural settings and generate theories from practice, second, a case study provides the means of answering the “how” and “why” questions to get more understanding of the phenomenon being studied and lastly, the case study enables the researcher to gain clear knowledge regarding the nature and complexity of process taking place. Equally this study intended to collect and analyze numerical data based on user requirements and facilitate the designing of the improved mechanism for detecting traditional-in-class examinations impersonations. This provided numerical patterns and statistical relationships within data, often focusing on measuring variables. To achieve these objectives expert review, cross-section survey approach and design science methods were applied. This implies that a mixed research methodology was

adopted during this study. Unlike longitudinal surveys which involve repeated measurements or observations of the same subjects or entities at multiple points in time this study applied a cross-sectional survey for collecting data from a single point in time, and thus it allowed for a researcher to collect data from groups of participants at one time point. Using a combination of methods provided a more comprehensive and insightful understanding of the research problem (Kothari, 2014). Also a mixed research methodology was helpful in assessing the effectiveness of an improved impersonations detection mechanism. For example, qualitative methods helped to uncover the experiences and perceptions of participants towards the use of the proposed impersonations detection mechanism, while quantitative methods was used to measure the systems outcomes and impact.

3.3 Study Area

This study was conducted in Tanzania where one public higher learning institution among 48 public higher learning institutions was selected (Tanzania Commission for Universities (TCU), Undergraduate Admission Guidebook, 2021/2022). The institution selected particularly The Mwalimu Nyerere Memorial Academy (MNMA) has three campuses one located in Dar es Salaam (main campus) while the rest are located in Zanzibar (Tanzania Island) where one campus is located in Pemba while another campus is located in Unguja. The criteria to select the study public higher learning institution was based on the availability of information regarding impersonations which was enough to attain the main objective of this study (Kobziev and Al Kilani, 2016). Also, MNMA is among of the top ten public higher learning institutions which is currently enrolling many students per annum. The current

enrollment is more than 14 000 students (enrollment report for 2023/24). This trend is not equivalent to the growth trend on the number of academic staff (academics), for instance, the Academy had 235 Academic staff for all her three (3) campuses (MNMA Prospectus, 2023/24). This number is equivalent to 1:60 lecturer to student ratio. Yet the Academy has observed repeated impersonations cases in three consecutive years (2020/21-2023/24). In reality, the number of reported impersonations cases at the Academy is not an actual number of impersonations cases committed by students during examinations because some of impersonators are passed undetected due to poor impersonations detection schemes prevailing at the Academy as it was revealed from the evidence reported by students who committed impersonations or observed impersonations at different times while they were passed unidentified. Results show that 10 (2.6%) respondents witnessed to have observed impersonators in the academic year 2022/23 and 13 (3.4%) respondents witnessed the same for the academic year 2023/24. This implies that impersonators witnessed by students are not equal to the number of impersonators detected by invigilators in examinations venues. In addition, a study conducted by Kobziev and Al Kilani in 2016 shows that a single case study is most applicable when the case is revelatory, represents a critical case for testing a formulated solution and is unique in nature.

3.4 Study Population

A study population is a group of persons, objects or items from which samples are drawn for research purpose (Mugo, 2009). The target population of this study was made up of academics, ICT officers, students, deputy rector academics, and academic directors. Therefore, the sample frame involved in this study is mainly

made up of academics with different sex, academic qualifications and years of examinations invigilation experiences; ICT officers with varied range of knowledge, skills and expertise in the area of human identification, and students. Also key respondents involved deputy rector and directors responsible for Academics. Table 3.1, and Table 3.2 illustrate the details of the population involved in this study.

Table 3.1: The Population of academics at the MNMA

Male	Female	Education Level			Total
147	88	Degree	Masters	PhD	
		32	139	64	235

Source: MNMA Prospectus, 2023/24

Table 3.2: Population of ICT staff at the MNMA

Male	Female	Area of Expertise			Total
		Programming	Network	Security	
5	1	3	2	1	6

Source: Field data, 2024

3.5 Sample Design

The sample frame involved in this study involved four heterogeneous groups namely students, ICT staff (experts), deputy rector and deputy directors responsible for academics. Due to the nature of the specified sample frame being heterogeneous in nature, a stratified random sampling method was applied to get the required sample size in each stratum. Sample selection method within two strata, namely the academics and students involved a simple random sampling method respectively while the rest of the strata namely the ICT staff (experts) and directors for academic involved a purposive sampling technique. The results of sample sizes calculations indicate that 148 academic staff (academics), 388 students; 1 director, 1 deputy

rector responsible for academics and 5 ICT experts were selected to create a total sample size of 543 from a population size of about 14 240 individuals with sampling error of 5% and 95% confidence level (Taro Yamane, 1968); (Patton, 2015); (MNMA Prospectus 2022/2023) and (Kothari (2014)).

The Taro Yamane equation ($n = N/1+Ne^2$); where n=sample size; N = Size of population and e = sampling error (5%) and 95% as the desired confidence level) was invoked to determine sample size for the academic staff and students strata respectively while a purposive sampling technique was employed in the rest of the strata. Table 3.3 shows the distribution of academic staff and students from the Academy. However, only 130 academics successfully responded on the survey questionnaire.

Table 3.3: The Number of Respondents

Category	Male	Female	Education level			Total
			Degree	Masters	PhD	
Academics	94	36	32	68	30	130
ICT Staff	4*	1*	2	2	1	5
Directors-Academics	2*	0	0	0	2	2
Students	132	256	388	0	0	388
TOTAL	232	293	422	70	33	525

Source: Field Data, 2024

Note: * represents conveniently samples

3.6 A Methodology for Developing an Enhanced NLP Model Which Detects Examinations Impersonations in PHLIS

Beside, to achieve the general objective of this study which was to develop an improved impersonations detection mechanism based on traditional-in-class

examinations in public higher institutions, the study had to apply an internationally accepted system development methodology known as “prototyping system development methodology” to implement the proposed solution prototype. The reason for adopting prototyping system development methodology was based on the fact that it is a very useful approach in improving the plan and implementing a software based research project (Garko and Ahmad, 2017). Prototyping methodology involves the development of a working system model known as a prototype for testing user requirements.

Therefore, the prototyping methodology was very useful in gaining more insight and experience in the new areas of the designed impersonations detection mechanism and new development technologies for further development. In addition, the prototyping system development methodology was very useful in evaluating the design, functionalities and system user interfaces of the designed mechanism. It was essential to show how user interacts with the implemented impersonations detection mechanism. As a result, prototyping helped both users and researcher validate and evaluate their requirements hence discover requirements that were omitted during requirements definition stage. The implementation of prototyping system development methodology involved several stages as the diagram in Figure 3.1 describes.

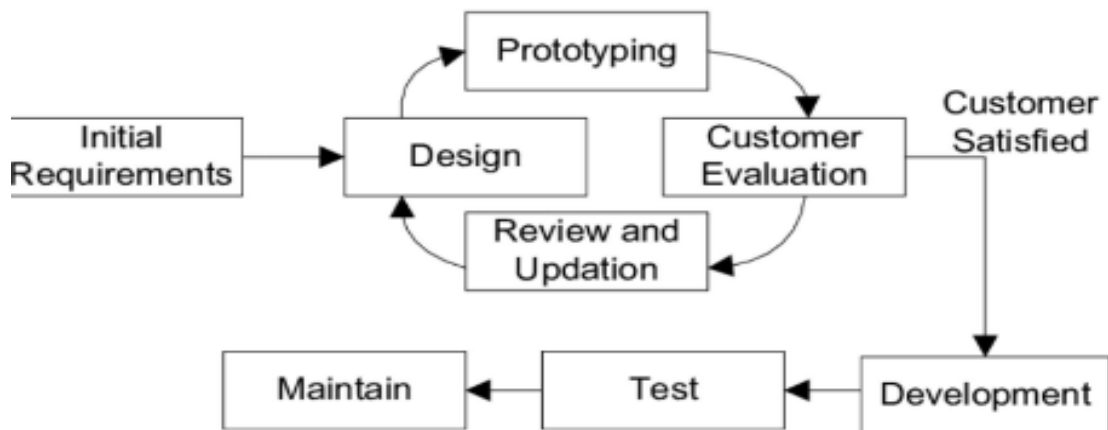


Figure 3.1: The Prototyping System Development Methodology

Source:<https://www.boardinfinity.com/blog/a-quick-guide-to-prototype-model-in-software-engineering/>

Moreover, the designed NLP model for generating DCQNS and facilitating the verification of students which in turn detects all incorrect entities as impersonators was developed by using three major frameworks which support the development of systems that are capable of processing natural language and machine learning logics. These frameworks include, flutter framework, Laravel Framework and the MYSQL database management system.

The Laravel framework was used to implement a web application due to its elegant syntax and modular packaging. The Laravel Framework follows the Model-View-Controller (MVC) architectural pattern, which provides a clear separation of concerns and helps organize code in a structured manner. Also the Laravel Framework include other feature suitable for implanting a suitable natural language processing model using different computer algorithms, these features include; a

Robust MVC Architecture, expressive syntax; built-in features and functionalities, support database migrations, Eloquent ORM (Object-Relational Mapping), form validation, queueing, task scheduling, and more; large Community Support; strong Security; supports multiple database systems out of the box, including MySQL, PostgreSQL, SQLite, and SQL Server (Database Agnostic); Blade templating engine; and the ability of the Laravel framework to offers seamless integration with popular third-party services and APIs through Composer packages and Laravel-specific libraries. Also the framework has Laravel package known as "milon/barcode" which facilitate the generation of QR code used by the client application to authenticate students. These features helped the developer to build powerful and feature-rich web applications quickly and efficiently (Setiawana, Suharjito and Diana, 2019) and (Richard, 2022).

Again a mobile application was developed to assists testing the designed natural language processing model which accomplish the task of student verification and impersonations detection. The mobile application was implemented with Flutter Framework which contains application interfaces (APIs) made up of restful development tools that communicate with application's backend (the server). Flutter was chosen due to its popular open-source UI software development kit created by Google, also Flutter support the building of a natively compiled applications for mobile, web, and desktop from a single codebase. It equally offers crucial features for implementing client-side applications, such features include Single Codebase, Multiple Platforms, offers a hot reload feature (Fast Development); Beautiful UIs, flexible design which allows for pixel-perfect customization and smooth animations;

Flutter applications are compiled directly to native machine code, resulting in high performance and faster startup times. Flutter also utilizes Skia, a powerful graphics engine, to render UI components, ensuring smooth performance across different devices; also flutter offers Access to Native Features; it has a growing community and ecosystem; flutter is backed by Google (Official Support from Google), supports Dart Programming Language that provide features like ahead-of-time (AOT) compilation and just-in-time (JIT) compilation for efficient application development; and provides Integration with RESTful APIs (Tashildar, Shah, Gala, Giri and Chavhan, 2020).

Moreover, a database side was implemented with MYSQL database management system due to various reasons including that MYSQL is an open source software, it is scalable, MYSQL has high performance, can efficiently execute complex queries and handle concurrent transactions, compatible with various operating systems such as Linux, Windows, macOS, and different programming languages like PHP, Python, Java, and all related languages, MySQL has a large Community Support, MySQL offers robust security features such as encryption, access controls, and authentication mechanisms to protect data from unauthorized access and ensure data integrity; as well as a mature and stable database system that has been used in production environments for many years (Domantas, 2024).

3.7 Research Design

Beside prototyping methodology, design science method was used to enhance the design process, improving the quality of design outcomes, addressing specific

design-related challenges and evaluating the designed improved impersonations detection mechanism based on traditional-in-class examinations. To facilitate an evaluation process, an expert survey method was used to gather opinions, insights, and judgments from individuals who possess specialized knowledge, expertise, and experience in the field of education, information and communication technology particularly in the area of impersonations detection techniques. This was very helpful as it facilitated the development of a very holistic solution based on such expertise and experiences.

3.8 Data Collection Methods

3.8.1 Data Collection Methods

Both primary data and secondary data were collected during this study. Studies identify several methods that were used for collecting data in this study, these methods include quantitative method (a survey questionnaire and demonstration) and qualitative method (an interview and document analysis) (Kothari, 2014) and (Garko and Ahmad, 2017).

3.8.1.1 Semi-structured Interview

The Interview method was selected due to its powerfulness in obtaining case study information and its cost effectiveness (Kothar, 2014). In this regards, a semi-structured interview was used due to its greater flexibility than other types of interview and it helped to explore more detailed information from the ICT officers and deputy directors and rector responsible for academics. Unlike structured interviews, which involve tight control over the format of questions and answers,

semi-structured interviews tend to contain open ended questions with emphasis being placed on the respondents for them to clarify points of interest (Denscombe, 1998). Also semi-structured interview helped to extract fresh explanations and important insights (Garko and Ahmad, 2017). The interview had a list of subjects in the interview guide from which the researcher expected to obtain answers from the respondents. The researcher allowed for both face and phone interviews and to a great extent flexibility in terms of restructuring questions as the case deemed necessary (Kothari, 2004) and (Kumar, 2005).

In this study, ICT staff and deputy directors and rector for academic were conveniently selected for interviews. 5 ICT officers were interviewed to solicit information regarding prominent impersonations detection technologies in the context of traditional-in-class examinations, their views on the proposed mechanism for detecting impersonations including the developed NLP model, components or features of the proposed mechanism for detecting impersonations, suitable frameworks for developing the NLP model and the system as a whole, usability and functional requirements of the proposed mechanism and criteria for evaluating the effectiveness of the proposed improved mechanism for detecting impersonations. Respondents were asked similar questions to obtain homogeneous information. The information gathered from these interviews with ICT officers and Directors/Rector for academics helped to confirm some findings from academics respondents and document analysis, ultimately helped to make accurate recommendations.

3.8.1.2 Survey Questionnaire

In the other hand, a survey questionnaire with both closed and open ended questions

was used to gather primary information from both Academic staff, ICT staff and Students. The questionnaire was developed in English language however questions were ad lipped to increase understanding that is, questions were clarified in Kiswahili language but with responses recorded in English language. As a result, a total of 130 academic staff responded to this survey, while 5 ICT staff accorded their responses to the survey as well. To ensure timely responses from respondents' online survey using Google forms was used to collect information from academic staff and ICT staff where online personal assistant using WhatsApp application and physical contacts were used for clarifying questions that required further interpretations. Precautions was taken to avoid element of bias. This helped to collect data with minimal cost and time. (saunder, 2007).

The survey questionnaire was used to collect data on sex, education level, campus, examinations invigilation experiences, awareness of impersonations fraud in the context of traditional classrooms examinations, trends of impersonations current impersonations detection methods or techniques and their limitations, perceptions on the need to embark into strengthening mechanism for detecting impersonations, recommendations on improvements that are to be made in the current impersonations detection methods or techniques in terms of time, efforts, cost, usability and technologies, information on relevant institution syndicate responsible for handling impersonations matters, the need of extra security officers during examinations and academic staff comfortability in using mobile technologies in improving impersonations detection strategies.

3.8.1.3 Secondary Data

Along survey questionnaire and semi-structured interview, a document analysis method was used to collect secondary data (Kothari, 2004). Garko and Ahmad (2017) identified three reasons for using document analysis in data collection: one document is used as input to the interview guide, it is also important in tracing the history of the organizations and its mission and vision, finally, it is helpful in lessening the biases of the interviews. Therefore, secondary data for this study was obtained from both print and electronic resources such as books, dissertations and electronic records from websites and online databases. The major points were summarized. Dissertations and reports related to this study gathered from the MNMA library where major sources of secondary information. Secondary information were helpful in enriching this study in two ways: The secondary sources enabled the researcher to make comparisons and establish trends through critical investigation of studies by showing the knowledge vacuum. Secondary sources enabled the researcher to gain experience by exploiting skills and knowledge of other researchers on the topic under study.

3.8.1.4 Demonstration

The developed system prototype was demonstrated and data from the demonstration was collected and analyzed to establish system performance, efficiency, security and convenience parameters.

3.9 Data Quality Control Management

Data quality was taken into an account to ensure the accuracy of information obtained from the respondents. This was achieved through the following ways:

3.9.1 Pre-Test

Data collection tools namely the survey questionnaire and interview were administered to few experts in the field of computer science to determine their validity and reliability (Ndunguru, 2017). Two experts were from the university in the Department of Math and ICT as well as some other two experts were selected from ICT department at the MNMA. Following expert review, some questions in the survey questionnaire and interview were amended and some were added to make them efficient to gather the required information and make them easy to understand. Again a mobile application was developed to test the working ability and efficiency of the developed model.

3.9.2 Triangulation

In this study, a combination of data collection methods was used to study some phenomena so as to ensure mutual agreements and confirmation of findings, more particularly data were collected through survey questionnaire and semi-structured interviews (Ridenour and Newman, 2008).

3.9.3 Ethical Considerations

Ethical issues refer to set of moral principles which provides rules and behavioral expectations about the most correct action towards experimental subjects and respondents (Best and Kahn, 2006). Research ethics provides researchers with a code of moral guidelines on how to conduct a research in acceptable manner. In this regard, this study observed a number of ethical issues throughout all processes. These include acquiring a research clearance letter from the OUT, and getting an

informed consent from the respondents. Respondents decided to participate in this study after getting informed on the purpose of this study and their voluntary involvement. It was clearly stated prior to actual data collection that this study was meant for academic purpose and that all the information from respondents would be treated confidentially without exposing respondents' identities in any way. Therefore, respondents were informed to use synonymous names whenever necessary.

3.9.4 Rigorousness

Survey questionnaire and interview guide were well structured to avoid ambiguous words so as to ensure that its questions were in line with research objective. Research was conducted very carefully for correct data collection and avoid biases.

3.10 Data Analysis and Presentation

Qualitative data from interview and documents were processed and analyzed by content analysis method and keyword extraction methods respectively while survey questionnaire and system demonstration results were organized, described, coded and analyzed through descriptive statistics and probability methods such as Frequency Analysis, measurement of percentages False acceptance rate (FAR) and false rejection rate (FRR) using survey analysis tool namely Statistical Package for Social Science version 16.0 and Google forms. Therefore, qualitative data from documents analysis and interview were used to supplement quantitative responses from survey questionnaire. Visualization methods such as bar charts and pi-charts, mobile application interfaces were used for data visualization. Cross tabulation was used to

enable the understanding of relationship between variables and the expert review report provided a better comparison of the field data. Finally, integration method was used to combine qualitative and quantitative findings to provide a more comprehensive understanding of the research questions. Results were presented by using various techniques such as tables, charts, system interfaces, flow charts, database design models, use case models, sequence diagrams and narrative explanations.

3.11 Performing Usability Test of the Developed Mechanism for Detecting Examinations Impersonations

The usability test was conducted by using real scenarios based on the implemented mechanism prototype. As a result, evaluating the usefulness of the implemented impersonations detection mechanism (system) was made possible. Usability test method always provides a mechanism for checking usable components of the system by placing its focus on human- computer interaction. False acceptance and false rejection methods were used to facilitate system prototype evaluation process. Also selected sample of 50 students (dataset) and 10 academic staff were allowed to interact with the designed mechanism prototype to evaluate its performance and efficiency. Suitable scale for evaluating the usability of the impersonations detection mechanism was adopted. The usability scale was based on 5, 4, 3, 2 and 1 for Strong disagree, to strong agree. Where a scale below 67% was considered as a concern which requires an immediate remedy (John, 2020). Also a risk based security assessment method was used to quantify the security level of the developed mechanism by using Abuse case scenarios. The abuse case scenarios are helpful in

identifying impersonations attacks when the implemented impersonations detection mechanism is being used to detect impersonations. Example of abuse case scenario involve a situation where students were allowed to exchange their life experience, then, be allowed to deceive an implemented impersonations detection system prototype. Results from the usability and security test was analyzed and interpreted to rich a final mechanism usability acceptance and implementation decision.

3.12 Summary

This chapter has described the research methodology used in this study. The study employed a mixed research methodology along with Prototyping approach in implementing the proposed improved mechanism for detecting impersonations in traditional-in-class examinations in Tanzania Pubic higher learning institutions. Academics and students were selected randomly where as ICT staff and top level managers responsible for academics were selected purposively. Survey questionnaire, mobile application and interview methods were employed to obtain primary data while document analysis method was used to obtain secondary data from books, journals, online databases, websites and reports. Descriptive statistics facilitated the analysis of survey data while content analysis facilitated the analysis of data from interview and documents. Additionally, SPSS version 16.0 and google forms facilitated descriptive analysis of the collected data.

CHAPTER FOUR

FINDINGS AND DISCUSSION

4.1 Introduction

This chapter presents and discusses findings driven from the analysed data which were collected from the study area and documentations. Findings presented here focus on responses to the research questions and specific objectives of this study. The main objective of this study was to develop an improved mechanism for detecting impersonations in the context of traditional-in-class examinations and it was based in Tanzania Public higher learning institutions where The Mwalimu Nyerere Memorial Academy (MNMA) was purposefully selected as a case study as details been described in Chapter 3. The study was focused on Academic staff, students, ICT officers, the deputy rector and directors responsible for academics research and consultancy (DR-ARC) where all decisions concerning examinations impersonations are taken care of.

Findings are presented inform of descriptions, tables, pie-charts, bar graphs and descriptive statistics. In addition use case diagrams, sequence diagrams, entity relationship diagrams, user interfaces and block diagrams are used for describing the functional requirements, system' objects interactions and database model of the proposed improved examinations impersonations detection mechanism. A mobile application has been developed to assess and evaluate the developed NLP model that performs impersonation detection exercise. The flow of findings and discussion are in line with the research objectives however preliminary sections present socio-demographic attributes and respondents perceptions on the states of impersonations

in Tanzania and The MNMA in particular. The remaining sections present themes reflecting research objectives.

4.2 Socio-Demographic Attributes of the Respondents

For the purpose of this study, respondents' socio-demographic attributes were important in providing the background of the respondents and their suitability for this study, they were also important in designing a user friendly NLP model for detecting impersonations at their institutions (Amide, Ladipo and Adebayo, 2015). In this regards, three socio-demographic attributes were captured and analysed including Age, education level, examinations invigilation experience and the area of expertise for the ICT officers. The findings on the attributes of the respondents are provided, analysed, interpreted and discussed in relation to their applicability to the subject under study. Respondents were asked to indicate their age, education level, examination invigilation experience and the area of expertise was included for the ICT officers whereas, details of findings are presented in section 4.2.1 through section 4.2.4.

4.2.1 Age of Respondents

In this study, age served as a crucial element to actively engaging individuals in the implementation process rather than merely studying them as passive subjects. The study respondents were requested to indicate their ages. The findings show that 29 (22.3%) of the academics were aged between 15 and 25 years, 59 (45.4%) of the academics were aged between 26-35, 29 (22.3%) of the academics were aged between 36 and 45 years, 12 (9.2%) of the academics were aged between 46 and 55

years while 1 (0.8%) of the academics was aged between 46 and 55 years and there was no academic who was above 65 years. Table 4.1 illustrates the details. On the other hand, result from the category of students show that 173 (44.6%) students were aged between 15 and 25, 120 (30.9 %) students were aged between 26 and 35 years, 60 (15.5 %) students were aged between 36 and 45 years, 30 (7.7 %) students were aged between 46 and 55 years and 5 (1.3%) students were aged between 56 and 65 years. Table 4.2 illustrates the details of ages for students.

The study findings on age indicate that most of the academic staff 129 (99.5%) who are the main user of the intended NLP model are of the age between 15 and 55 and most students 353 (98.6%) who actually access the proposed NLP model very rarely are of the age between 15 and 45 years. Age analysis implies that respondents' age is the age between youth and elderly people who actively engage in using ICT products such as mobile phones and its enablers. It has been noted that most human computer interaction (HCI) researches dedicated to applications for which target users are known or can be reasonably well defined take age of users into an account. Brouwer-Janse et al (1997) in their article of "user interface for the young" describe that computer applications that target aged people must aim at enhancing mobility, independency and social participation. Aged people need to maintain an active role in the community to be able to use and enjoy the benefits of technological innovations for long as possible. Computer products such as software and hardware should play a major role in achieving this aim and this can be achieved only if these products meet age requirements of the user.

Table 4.1: Distribution of Respondents (Academics) by Age

Age Interval	Frequency	Percentage
15-25	29	22.3
26-35	59	45.4
36-45	29	22.3
46-55	12	9.2
56-65	1	0.8
Above 65	0	0.0
TOTAL	130	100

Source: Field Data, 2024

Table 4.2: Distribution of Respondents (Students) by Age

Age interval	Frequency	Percentage
15-25	173	44.6
26-35	120	30.9
36-45	60	15.5
46-55	5	1.3
Above 55	0	0.0
TOTAL	358	100

Source: Field Data, 2024

4.2.2 Education Level of Respondents

Education levels and expertise of the respondents were important in knowing the acceptance of modern impersonations detection models, model development expertise and recommendations for the improved impersonation detection practices. Abu-Shanab (2011) argues that, the more educated individual are the more is the acceptance of a new technology. Therefore, it was imperative to establish the education level of academics that are involved in examination invigilation activity using the proposed NLP model. In response to education level attribute, respondents were asked to indicate their education levels whereas, the findings indicate that majority of academics 119 (91.6%) had at least first degree whereas majority of ICT

Officers (100%) were graduates in the field of computer such as Computer Science, Information Technology and Computer Engineering and had different expertise including computer programming, computer security and software development skills. Also all students 353(100%) were undertaking studies in different Ordinary Diploma and degree programmes. Summary of the information regarding education level of academics and ICT officers as well as impersonation awareness among academics is presented in Table 4.3, Table 4.4 and Figure 4.1.

Table 4.3: Education Level of Academics (n=130)

Education Level	Frequency	Percentage
Basic Technician Certificate (BTC)	1	0.7
Technician Certificate (TC)	2	1.5
Ordinary Diploma (OD)	8	6.2
Bachelor Degree (BD)	32	49.2
Postgraduate Diploma (PD)	4	3.1
Master's Degree (MD)	69	28.5
PhD	14	10.8
TOTAL	130	100

Source: Field Data (2024)

Table 4.4: Education Level of ICT Officers (n=5)

Education Level	Computer Programming	Computer security	Software development	Total
Bachelor Degree	2	1	2	5

Source: Field Data (2024)

4.3 Academics' Awareness and Perception on the Concept of Impersonations

This part presents respondents views on their understanding of the concept of impersonations. Most respondents (both academics and ICT Officers) were aware of the concept of impersonations thus helped to get valid responses from the field.

Figure 4.4 shows the responses of academics on the awareness of impersonations in higher learning institutions where as 90% of academics were aware of the impersonations concept.

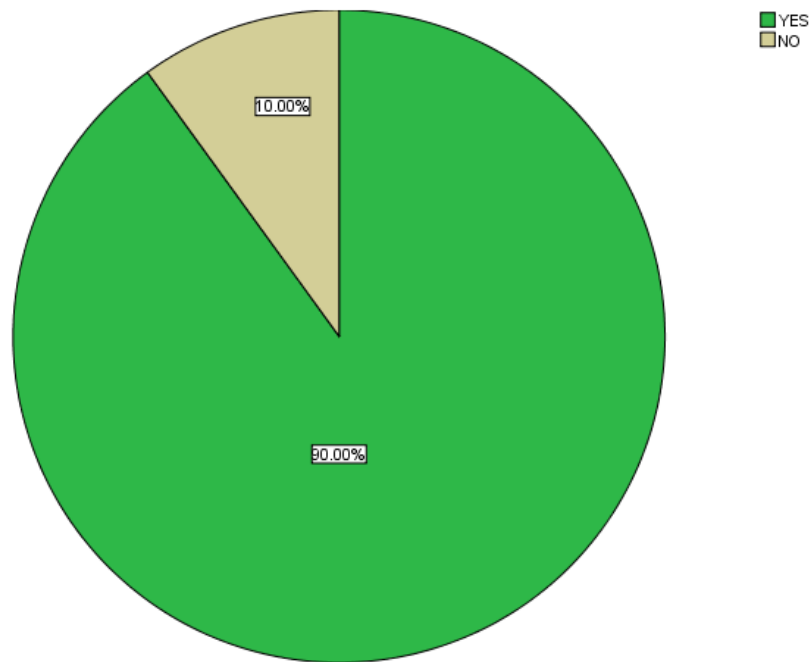


Figure 4.1: Impersonations Awareness Among Academics

Field Data, 2024

4.4 Prominent Impersonations Detection Technologies in Traditional-In-Class Examinations in Public Higher Learning Institutions

Impersonations in the traditional-in-class examinations environment can pose significant challenges to maintaining academic integrity and security. As technology continues to evolve, various machine learning models have been emerged to detect and prevent such fraudulent activities. This study aimed to identify prominent technologies utilized by academics for detecting impersonations during examinations

in Tanzania Public higher learning institutions and beyond based on traditional-in-class settings and discuss their effectiveness and potential implications. The study assessed ICT officers and academics knowledge and understanding of impersonations detection technologies in traditional—in-class examinations in public higher learning institutions before they could actually identifying the prominent impersonations detection technologies in same context. Thus, section 4.4.1 presents respondents' knowledge and understanding of impersonations detection technologies; section 4.4.2 explain the method used to collect information from academics and ICT officers, section 4.4.3 dwells on the identified prominent technologies used for detecting impersonations in the context of traditional –in-class examinations based in Tanzania public higher learning institutions as described by academics, ICT officers and literatures related to this study whereas section 4.4.4 presents discussion and section 4.4.5 entails summary of this section (section 4.4).

4.4.1 Methods Used to Collect Information from Academics and ICT Officers Regarding Prominent Impersonations Detection Technologies

To achieve the objective of identifying prominent technologies for detecting impersonations in the context of traditional-in-class examinations in public higher learning institutions, a broad document review was conducted focusing on technologies specifically designed for detecting impersonations in traditional-in-class environments. Relevant academic databases, journals, conference proceedings, and reputable online sources were explored to gather pertinent information. Keywords such as "impersonations detection," "traditional classroom," and "academic integrity" were used to filter the search results. In addition, a survey questionnaire was supplied

to the selected 130 academics and a semi-structured interview was conducted with 5 ICT officers, deputy rector and deputy director for academics. After a careful evaluation, technologies with significant relevance and impact were selected for inclusion in this study report.

4.4.2 Respondents' Knowledge and Understanding on Impersonations Detection Technologies

Academics and ICT officers were asked to indicate whether they were aware of impersonations detection technologies in public higher learning institutions. Majority of them 117 (90%) indicated to be aware of impersonations detection technologies being used in public higher learning institutions' traditional-in-class examinations environment, however the minors 13 (10%) indicated to lack such important knowledge and understanding. The findings is presented in Figure 4.2.

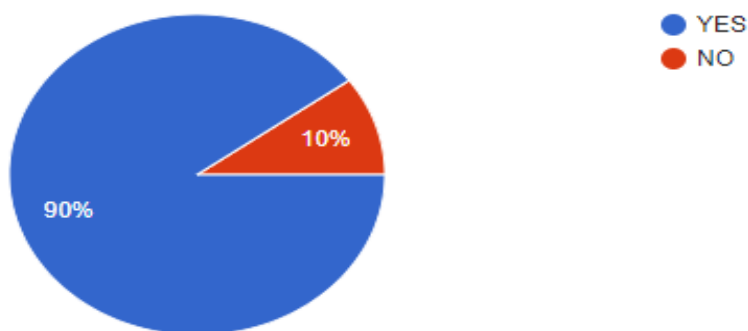


Figure 4.2: Respondents' Knowledge and Understanding on Impersonations Detection Technologies

Findings signify the high level of knowledge and understanding on the impersonations detection technologies among academics and ICT officers which is

attributed by the fact that ICT officers had expertise in the study area while academics had higher education which enabled them to interact with various user identification technologies at work and during studies. These findings concur with finding from a study conducted by Elizabeth and Zira (2009) on farmers' awareness on agricultural technologies which is attributed by their levels of education. Abu-Shanab (2011) argues that knowledge and understanding on technologies enables people to utilize best technologies in solving particular social problems. Respondents' knowledge and understanding on prominent impersonations detection technologies facilitated them to recommend appropriate technologies and helped the researcher to gain insight in technologies suitable for developing an enhanced NLP Model which detects impersonations based on the context of relevant entity. Also it suggests that respondents were able to highlight prominent impersonations detection technologies surrounding their institution.

4.4.3 Prominent Technologies for Detecting Impersonations in the Context of Traditional –in-Class Examinations in Tanzania Public Higher Learning Institutions

Academics and ICT officers were asked to state technologies for detecting impersonations in the context of traditional –in-class examinations in Tanzania public higher learning institutions. As Table 4.5 illustrates. 20 (15.4%) of the responding academics identified QR code technology; 5 (3.8%) of the responding academics identified Biometric Authentication Systems; while 1 (0.8%) of the responding academics identified Behavioral Analysis tools. In the other hand, 18 (13.8%) of the responding academics identified Proctoring Software; 2 (1.5%) of the

responding academics identified Machine Learning-Based Approaches and 74 (57%) of the responding academics identified a combination of more than one approach such as a combination of QR code technology and Profile based static questions whereas, 10 (7.7%) respondents identified traditional methods such as examination coupons and student identity cards. Responses from the interview conducted with ICT officers concurred with the former responses presented by academics however their suggestions had comprehensive technical descriptions and recommendations.

Table 4.5: Prominent Technologies for Detecting Impersonations in the Context of Traditional –in-class Examinations in Tanzania Public Higher Learning Institutions Identified by Academics (n=140)

Technology	Frequency	Percentage
QR code technology	20	15.4
Biometric Authentication Systems	5	3.8
Behavioral Analysis tools	1	0.8
Proctoring Software	18	13.8
Machine Learning-Based Approaches	2	1.5
Combination of more than one approach such as a combination of QR code technology and profile based questions	74	57
Traditional Identity Cards	10	7.7
TOTAL	130	100

Source: Field Data (2024)

Furthermore; findings from the semi-structured interview conducted with 5 ICT Officers established the details for the identified impersonation detection technologies as presented in section 4.4.3.1 through section 4.4.3.5

4.4.3.1 Facial Recognition Technology

Facial recognition technology has gained traction as an effective tool for identifying individuals in various contexts, including educational settings. In traditional classrooms, facial recognition systems can be deployed to verify the identity of students during examinations or assessments. These systems capture and analyze facial features to authenticate students, thereby minimizing the risk of impersonations. However, concerns regarding privacy, accuracy, and ethical considerations have been raised, necessitating careful implementation and oversight. In support of these contentions Ahmed (2022) contends that Facial recognition technology poses numerous privacy and security concerns, including issues like absence of consent, unencrypted facial data, and lack of transparency, technical vulnerabilities, and inaccuracies.

4.4.3.2 Biometric Authentication Systems

Biometric authentication systems, such as fingerprint scanners and iris recognition technology offer another layer of security in detecting impersonations. By linking unique biometric identifiers to individual students, these systems ensure accurate identification and prevent fraudulent behavior. However, challenges related to scalability, cost, and user acceptance may limit widespread adoption in physical classroom environments. Similar challenges were also presented by Adigun and Yekini (2012) in their study titled ‘A Biometric Model for Examination Screening and Attendance Monitoring in Yaba College of Technology’.

4.4.3.3 Behavioral Analytics Tools

Behavioral analytics tools monitor and analyze students' behavioral patterns during classroom activities to detect anomalies indicative of impersonations or cheating. These systems utilize data from various sources, such as attendance records, keystroke dynamics, and mouse movements, to establish baseline behavior and identify deviations. While behavioral analytics can provide valuable insights into students' interactions and engagement, concerns regarding privacy and data security must be addressed.

4.4.3.4 Proctoring Software Platforms

Proctoring software platforms equipped with features such as live monitoring, screen recording, and identity verification, are increasingly being employed to deter impersonations during examinations. These tools allow instructors to remotely supervise students in real-time and intervene if suspicious behavior is detected. However, criticisms regarding invasiveness, accessibility, and efficacy have sparked debates surrounding their ethical implications and practicality.

4.4.3.5 Dynamic Challenging Questions Based on Student's Profiles

Results show that dynamic challenging questions (DCQNs) based on student's profiles can be an effective method for user identification and impersonations detection, particularly in scenarios where traditional methods like passwords or biometrics may not be sufficient. In addition respondents highlighted students' background information such as names, date of birth, parents or guardian's information, area of domicile and other similar student's information as a base for

creating a model that generate dynamic challenging questions tailored to different students' profiles. Authors who support dynamic challenging questions as a base of user identification present that this approach can be used in various industries and applications where authentication and security are paramount. Some common areas where this approach has been employed include: Online Banking and Financial Services, E-commerce and Retail, Healthcare and Telemedicine, Educational Institutions and other industries where the verification of the identities of entities before accessing services is necessary (LoPuck, 2002).

4.4.4 Discussion

The findings suggest that a combination of technologies, tailored to the specific needs and constraints of traditional-in-class environments, may offer the most effective approach to detecting impersonations. A hybrid approach (model) such as a combination of QR code and dynamic challenging questions provides robust mechanisms for verifying students' identities and detecting impersonations, while behavioral analytics and proctoring software offer insights into students' behaviors and activities. However, it is essential to strike a balance between security measures and students' rights to privacy and dignity. Moreover, ongoing research and development are needed to address the limitations and challenges associated with implementing these technologies in higher educational settings.

4.4.5 Summary

Identifying and implementing the identified prominent technologies for detecting impersonations in traditional-in- class examinations environments is crucial for

upholding academic integrity and ensuring fair assessment practices. Facial recognition, biometric authentication, behavioral analytics, and proctoring software represent promising solutions, although with inherent limitations and ethical considerations. A hybrid approach such as a combination of QR code technology and dynamic challenging questions approach provides robust mechanisms for verifying students' identities and detecting impersonations with minimum cost. Moving forward, interdisciplinary collaboration and stakeholder engagement will be essential to navigate the complex landscape of technology-enabled impersonations detection while safeguarding students' rights and promoting a culture of academic honesty. This section has provided valuable insights into the current state of technologies for combating impersonations in traditional-class examinations and sets the stage for future investigations and innovations in this field.

4.5 Developing an Enhanced Natural Language Processing (NLP) Model for Detecting Impersonations in the Context of Traditional-In-Class Examinations in Tanzania Higher Learning Institutions

4.5.1 Introduction

This section presents findings of the results from survey questionnaire administered to academics document analysis and semi-structured interview conducted with ICT officers' who actually possesses mixed experience in the field of impersonations detection techniques including NLP algorithm and its techniques. The effort was focused on research objective that intended to develop an enhanced model which utilizes the NLP algorithm and Question Generation (QG) technique for detecting impersonations in examinations. This is a hybrid implementation of impersonation

detection mechanism which integrates dynamic challenging questions technique and the QR code authentication approach. The enhanced NLP model requires students to register or enroll in the proposed verification system before an actual identification process. This helps to build a huge data structure (dataset) which is utilized by the proposed model to create dynamic challenging questions randomly and present them to the user via a mobile application interface along with questions corresponding answers. The enhanced NLP model requires students to provide questions' corresponding answers to verify their identities and eligibility to access examinations venues. To discourage students from sharing answers to a third part, the NLP model creates a set of challenging questions dynamically and randomly based on students' profile that is held in the student database system.

4.5.2 Identifying Suitable Mechanism (Technique) for Detecting Impersonations in Traditional-in-class Examinations in Tanzania Public Higher Learning Institutions

It was sought to establish the suitable mechanism for integrating relevant techniques that could improve the detection of impersonations in the context of Tanzania higher learning institutions traditional-in-class examinations context. In this regards, respondents were asked to select the most suitable combination of impersonations detection techniques that fits in their institutional setting. The results summarized in Table 4.6 indicate that 70 (53.8%) of academics selected a combination of QR code and a dynamic challenging questions generation based on student's' profile technique to create a robust NLP model that perfectly detects impersonations, 10 (7.7%) of academics selected a combination of biometric techniques such as a

fingerprint and dynamic challenging questions approach to detect impersonations and 15 (11.5%) of academics selected a combination of biometrics (a bi-model) approach to detect impersonations. Again, 12 (9.2%) academics selected a combination of a near field communication (NFC) cards and dynamic challenging questions based on student's profile approach to detect impersonations while 23 (17.8%) of academics selected a combination of bar code and dynamic challenging questions based on student profile approach to detect impersonations. In the other hand, findings from the interview conducted with 5 ICT officers indicate that 4 (80%) respondents suggested that a combination of the QR code technique and dynamic challenging questions based on student's profile approach could be an effective model for impersonations detection particularly in scenarios where traditional methods like passwords or biometrics may not be sufficient. This suggestion concur with the option selected by majority (53.8%) of the academics. However 1 (20%) ICT officers suggested a combination of NFC cards and dynamic challenging questions based on student profile approach to detect impersonations (Tables 4.6 and 4.7). Furthermore, respondents stated that these dynamic challenging questions can be tailored to students' profile which contains information such as names, course results, tutors' information, parents or guardians' information, place of birth and all related information to providing an additional layer of security and personalization to the identification process. In addition, a study conducted by Ullah, Xiao and Barker (2018), "A Dynamic Profile Questions Approach to Mitigate impersonations in Online Examinations" found that using a dynamic challenging questions based on user profile has a significant increase in impersonations detection effectiveness of about 99.5%. Also using profile questions to identify people is a

robust and reliable method for human identification as suggested by LoPuck (2002) in the theory of human identification.

Therefore based on these findings, it was established that implementing the hybrid model which combine dynamic challenge questions based on student profile approach and the QR code technology is best implementation for improving impersonations detection mechanism in Tanzania public higher learning institutions. However, a model which combines dynamic challenging questions based on student profile and QR code requires careful consideration of various requirements to ensure effectiveness, security, and usability. Such considerations include user profile data collection; Data Security and Privacy (encrypt data); model development which ensures that the generated questions are dynamic, random, diverse, relevant, and tailored to individual students' characteristics and preferences. Questions relevance and difficultness produces an intuitive and user-friendly interface for answering dynamic challenging questions. Also, with randomization, questions variation and presentation of challenging questions prevents predictability and minimize the risk of fraud.

Table 4.6: Academics Responses on the Improved Impersonations Detection Approaches

Impersonations detection approach	Frequency	Percentage
A combination of QR code and dynamic challenging questions based on student profile	70	53.8
A combination of biometrics such as fingerprint and dynamic challenging questions based on student profile.	10	7.7
A combination of biometrics (a bi-model).	15	11.5
A combination of NFC cards and dynamic challenging questions based on student profile.	12	9.2
A combination of bar code and dynamic challenging questions based on student profile.	23	17.8
TOTAL	130	100

Source: Field Data (2024)

Table 4.7: ICT Officers Responses on Impersonations Detection Approaches

Impersonations detection approach	Frequency	Percentage
A combination of QR code and dynamic challenging questions.	4	80
A combination of biometrics such as fingerprint and dynamic challenging questions.	0	0
A combination of biometrics and dynamic challenging questions.	0	0
A combination of NFC cards and dynamic challenging questions.	1	20
A combination of bar code and dynamic challenging questions.	0	0
TOTAL	5	100

4.5.3 Proposed System Architecture of the Improved Mechanism for Detecting Impersonations in Traditional-In-Class Examinations in Tanzania Public Higher Learning Institutions

Apart from suggesting a suitable mechanism which would improve impersonations detection in traditional-in-class examinations, a researcher was interested to establish the components (features) of the proposed approach. To achieve this objective, a

document analysis along with semi-structured interview exercise were undertake. The semi-structured interview was conducted with 5 selected ICT officers from the MNMA. Findings from the interview indicate that QR code scanner such as a cross-platform mobile application, questions generation algorithm and technique, attendance taking technique, database of users as well as system communication technique are of paramount importance in designing the NLP model which detects examinations impersonations.

In the other hand, a list of questions were administered to academics requesting them to indicate the relevant institution syndicate where impersonations irregularity is submitted for further proceedings. 47 (37.6%) of the respondents indicated that impersonations irregularity is reported to the office of deputy rector academic, research and consultancy (DR-ARC) while 52 (41.6%) indicated that similar report is submitted to the examination department while 11 (8.8%) indicated that same information is communicated to the department of the respective impersonator and 53(42.4%) indicated that impersonations irregularity is reported to both DR-ARC, head of department and examination department, also 7 (5.6 %) indicated that same information is communicated to the admission office where 6 (4.8%) indicated that the similar information is communicated to security office (Figure 4.3 shows these results). Given the discrepancies in the responses provided by the academics regarding to where impersonations report is communicated, an interview was conducted with the deputy rector academics, research and consultancy (DR-ARC) who takes charge of all academic matters including examination impersonations. The DR-ARC indicated that all examination irregularity matters including impersonations

are reported to examination office which produce relevant report to his office and that it is in the mandate of his to appointing an ad hoc committee that takes charge of the reported examination irregularity. Further evidence to where examination irregularities are reported at the MNMA can be found in the examination regulations and guidelines book published by the Academy in 2024 (available in softcopy at www.mnma.ac.tz).

These findings suggest that a proposed impersonations detection model should take into an account of where impersonations report should be reported, particularly in the examinations office.

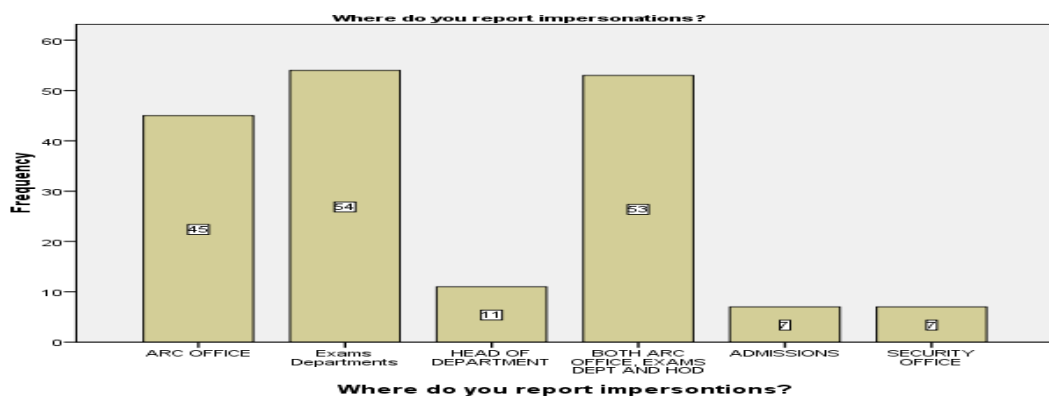


Figure 4.3: Respondents' Responses to the Institution Syndicate where Impersonations are Reported

Source; Field Data, 2024

In the other hand, a researcher was interested to establish whether academics had witnessed any act aiming at harming an invigilator during examinations sessions and if an institution provides security officers to the examination rooms during examinations who should take care of security matters that could arise. Findings from the survey questionnaire (see Figure 4.4) indicate that majority of the

respondents 63 (51.2%) agreed to have witnessed an event where the impersonator tended to harm the invigilator. In addition, some concern revolves around the fear of encountering impersonators in the examination room. For instance, during an interview, one respondent, whose identity remains undisclosed for security reasons, recounted an incident from one year ago (in 2023) where an invigilator apprehended an impersonator at examination venue X (name of the venue reserved). The impersonator attempted to physically harm the invigilator in an effort to flee the scene of impersonations and tamper with evidence. The respondent emphasized the critical importance of having a nearby security officer present to ensure the safety of both invigilators and other students, including potential impersonators. Furthermore, findings from the interview conducted with deputy director for academics at Pemba Campus revealed another theme of interest that the owed impersonations detection model should facilitate students' attendance recording during students' verification rather than relying on the current manual attendance taking method. "This can save invigilation time and efforts as well as increase more attention to examinations invigilation rather than taking some time to take students attendance", the respondent added. The idea of automated attendance taking during examinations is equally supported by findings from studies conducted by Abdullahi Nura and Jiya (2019) in their study entitled "Examination Eligibility Verification and Attendance System Using Quick Response Code" and the study by Odejobi and Clarke (2009) "Implementing Biometrics to Curb Examination Malpractices in Nigeria".

These findings suggest that the proposed impersonations detection model should incorporate a module for communicating with the security office to notify them

through voice calls or Short Message Service (SMS) in the event of impersonations detection for them to take care of security matters around particular examinations venue and that the model should include a mechanism for recording students attendance during an examination eligibility verification exercise.

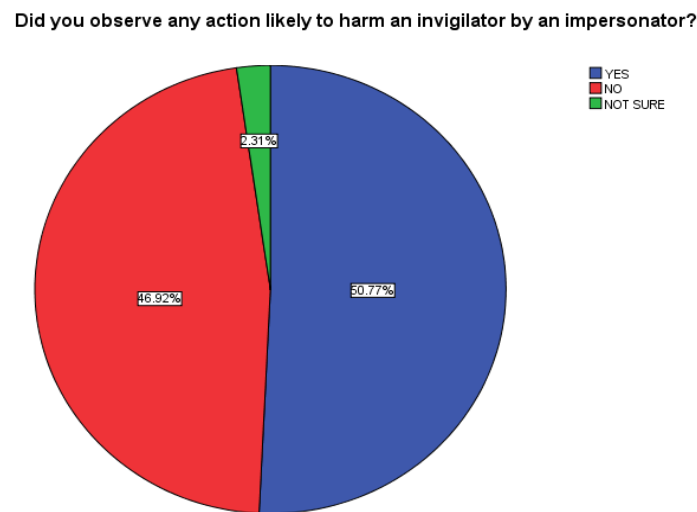


Figure 4.4: Academics Response on Witnessing Action Tendered by an Impersonator that Aimed at Harming the Invigilator

Source; Filed Data, 2024

4.5.4 Summary

In regards to the findings from section 4.5.3, the enhanced NLP model for detecting impersonations in traditional-in-class examinations in public higher learning institutions should include seven major components or modules namely: a user's registration module, QR code generation, questions generation technique, impersonations detection technique, attendance taking, system communication system reports generation mechanism. Users of the proposed solution include

students, invigilators, examination officers, heads of academic departments, security officers and the system administrator.

4.5.5 Designing the Enhanced NLP Model for Generating Dynamic Challenging Questions Based on Stunt's Profile

The researcher was interested to establish the working mechanism of the proposed NLP model (which integrates QR code technique and dynamic challenging questions based on student profile technique) and set criteria for evaluating the implementation of an application (system) that implements the designed NLP model. This was achieved through requirements engineering process and a prototyping system development methodology.

To gain considerable approval for the research, a globally recognized software engineering model and a NLP algorithm along its Question generation technique were employed. The NLP algorithm was selected due to its Enhanced Security since the dynamic questions are generated on-the-fly by an NLP model, are unique and unpredictable, making it harder for unauthorized users to guess or retrieve answers; also NLP models can adjust the complexity of questions based on user interaction patterns, ensuring that questions are neither too simple to guess nor too complex for legitimate users to answer (adaptive complexity; NLP models can generate questions that are contextually relevant to the user (Personalization and Relevance); and NLP models can generate questions in natural language, making the interaction feel more intuitive and less intrusive (Enhanced User Experience). Consequently, the system showcasing the suggested enhanced NLP model was crafted utilizing the prototype

model, known for its object-oriented approach to system development. The utilization of the prototyping system development model enhanced both the planning and execution phases of the system prototype. It involved creating an executable software system (prototype) for testing purposes, which proved highly beneficial for gaining hands-on experience in new areas of the system describing the proposed NLP model and facilitated the evolutionary development of the NLP model. Additionally, employing a prototype system development methodology aided in evaluating the proposed model design, functionalities, and user interactions.

Consequently, it was found out to be useful in redefining certain system (model) specifications that were initially perceived as well-defined. However, when users actually attempted to use the system (model), they discovered that their needs had not been adequately captured. Hence, the prototype facilitated users in validating and evaluating their requirements, uncovering any omissions in requirements at an early stage in the process. This, in turn, assisted the researcher in gaining a deeper understanding of the users' needs and the model development techniques involved. It also provided an opportunity for the users to explore various possibilities and investigate the feasibility of the proposed system. A diagram in Figure 4.5 describes the major stages executed while developing the proposed impersonation detection system whereas Figure 4.6 describes the phases adopted in developing the enhanced NLP model for detecting impersonations. Details for the enhanced NLP model are shown in section 4.5.5.1.

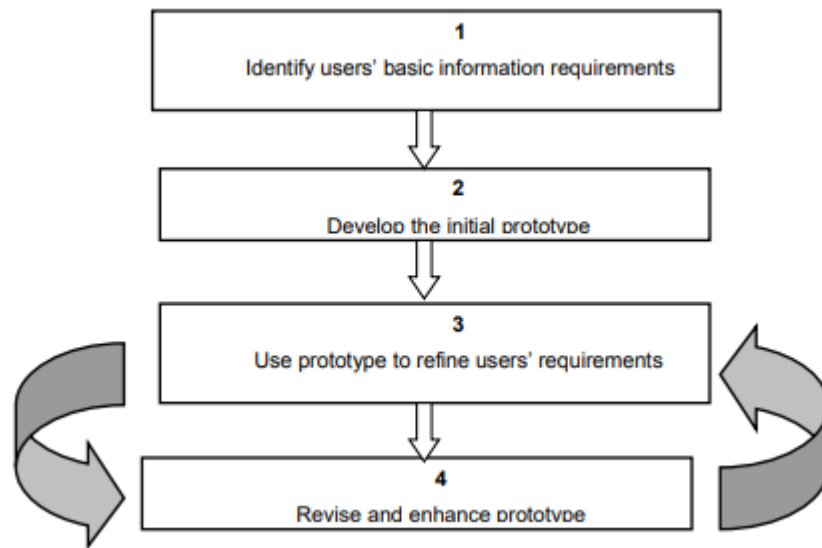


Figure 4.5: Development of the Proposed Improved Impersonations Detection System

Source: draw.io

4.5.5.1 Implementing the Proposed Enhanced NLP Model for Detecting Examinations Impersonations as Shown in Figure 4.6

Creating a set of dynamic challenging questions to verify the identity of a student that in turn facilitate the detection of impersonations typically involves generating personalized questions based on the student's unique information. To achieve this goal a knowledge-based authentication (KBA) approach was analysed and implemented. KBA relies on information that the student is expected to know, often derived from their personal or academic history. The implantation of KBA was achieved by using a Natural Language Processing (NLP) algorithm and Question Generation (QG) technique due to various factors including that NLP can handle both structured and unstructured data, making it versatile in generating questions from diverse types of student information know as Flexibility, advanced NLP models

can generate a wide variety of questions, making them less predictable and more challenging, NLP techniques, especially with models like GPT-4 or BERT, can understand context and generate more natural and relevant questions as well as NLP can generate highly personalized questions by interpreting complex and varied datasets. However NLP poses some challenges that requires serious considerations such as NLP models can be complex to develop and require significant computational resources (complexity), they often require large amounts of training data to perform well and generating questions dynamically can be slower compared to the rule-based approach of Decision Trees. Thus a Question generation technique was used to carefully design the NLP model that adequately detects impersonations with great accuracy and reasonable amount of dataset. The next section below presents the NLP model implementation steps and detail.

4.5.5.1.1 User Enrollment

During the enrollment phase, the user (students, heads of departments and invigilators) were asked to provide necessary information which was stored securely in the system database to make the model training and model testing dataset. Student information included but not limited to personal details, academic records, previous schools information and next of kin information. Student information were collected together to form individual student profile which is trained to the NLP model to generate personalized dynamic challenging questions.

4.5.5.1.2 QR Code Generation

The proposed NLP model is linked with a QR code generator in which when a

student needs to be verified the QR code generator generates QR code that encodes a unique session identifier (student registration number) and URL leading to the KBA system (student authentication system).

4.5.5.1.3 Authentication Process

QR Code Scanning initiate the authentication process where by an invigilators scans the QR Code using their mobile device installed with an authentication model (application). Upon scanning, the system retrieves registration number from the QR code. Then the system initiates the KBA process using the registration number. The system creates a set of dynamic questions based on the student's stored information. Samples of dynamic questions generated include questions like "What grade did you receive in Database Course?", "Who was your instructor for database management system?" and "What is the last name of your next of kin?"

The next step involve presenting generated questions to the user on their mobile device system interface which is monitored by an invigilator whereas an invigilator collect answers from students and validate them with answers generated by the system. If the answers match, the invigilator command the system to verify student and keep log file of all verified students which is treated as an attendance sheet.

4.5.5.1.4 Feature Extraction

The model extracts relevant features from the collected data using Question

generation (QG) technique. The technique involves identifying key entities such as course names, grades, project titles, and dates of birth where an entity extraction process highlight key features from the data.

4.5.5.1.5 Model Training

The NLP model was trained on the collected and processed data to generate questions. This involved feeding the model with question syntax and learning how to generate appropriate questions.

4.5.5.1.6 Template Design

To ensure that the questions are both relevant and varied a template for questions generation that can be filled dynamically with the extracted features was designed.

4.5.5.1.7 Evaluation

Then the generated questions and answers were evaluated to ensure they are challenging and accurate. It involved human oversight to make some suggestions based on the generated questions and answers by the model.

4.5.5.1.8 Dynamic Challenging Questions (DCQNS) Presentations

The DCQNS generated by the system were presented on a mobile device screen showing a question with dynamic placeholders filled in (e.g., "What grade did you receive in Data Structures?") along with it corresponding answer.

4.5.5.1.9 Impersonation Detection

The system provides a check button indicating to confirm student eligibility or an

impersonation and produces successful verification message when the button is activated. In the event of impersonation detection the system generates an SMS which is then sent to a security officer via his mobile phone to let him attend the incidence.

The pictorial representation in Figure 4.6 encapsulates the flow from data collection through to the dynamic challenging questions generation and presentation of questions for student identity verification and impersonation detection in the developed NLP model.

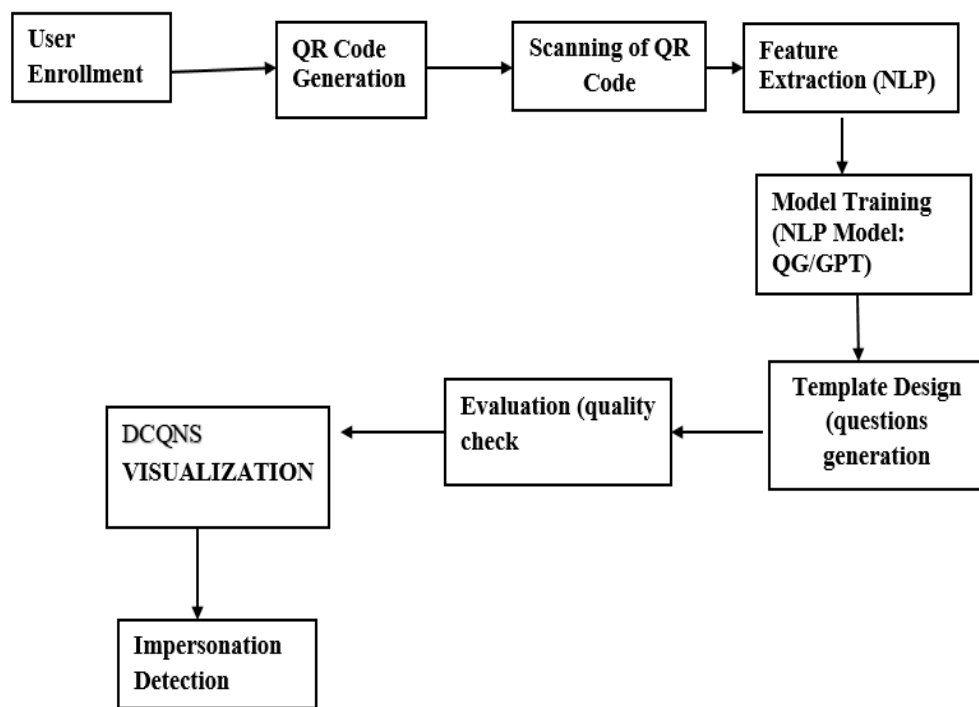


Figure 4.6: Phases for the Proposed Enhanced NLP Model for Detecting Examinations Impersonations

Source; Drawn in MS. Word

4.5.5.1.10 Summary

Therefore; this section described the designed and developed enhanced NLP model which detect examinations impersonations. The novel contribution of this model in classroom security is due to an innovative use of NLP to enhance academic integrity and security in physical classrooms, addressing impersonations which is often overlooked in traditional authentication methods. The model integrates QR code based authentication technique and dynamic challenging questions generation technique to effectively and timely detect impersonations in traditional-in-class examinations. Unlike static authentication methods, this approach leverages dynamically generated profile questions that adapt based on historic data, making impersonation detection more robust and contextually intelligent. Authors that support using dynamic challenging questions for user identifications include Ullah, Barker and Xiao (2017); Ullah (2017); Ullah, Xiao, Lilley and Barker (2012) and Ullah, Xiao, Lilley and Barker (2014). These studies discovered various security and usability concerns such as: the text based questions were less usable as they could be predicted, some questions could be easily guessed and this was seen as security vulnerability, image based questions were more effective than text based questions due to the ability of memorizing image and use objective questions such as multiple choice questions, students could share pre-defined text and image based questions to the impersonator. In the other hand studies found out that the more the questions are shared is the more success of an impersonations attack.

Conversely, the bigger the size of student profile the more it is difficult to predict questions hence more effective in impersonations detection. With respect to

impersonations attack described in several studies identified in previous paragraphs, respondents' responses on students profile based questions to detect impersonations and issues raised above regarding the use of text based and image based challenging questions, this study proposed a dynamic challenging questions based on a detailed student profile. Equally dynamic challenging questions are well supported by several authors including Ullah Xiao and Barker (2019).

4.5.5.2 A mathematical Representation on the Technique for Generating Dynamic Challenging Questions

To provide a mathematical representation of how Question Generation (QG) technique uses student information to create dynamic challenging questions along with their corresponding answers for identity verification, the process was broken into several key components: data extraction, question generation, and answer extraction. Here's a step-by-step mathematical representation:

Step 1: Data Extraction

Let D be the dataset (database) containing the student's information, which includes various entities such as courses, grades, programme name, and dates.

$$D = \{(e1, v1), (e2, v2), \dots, (en, vn)\}$$

Where ei represents an entity type (e.g., "Course Name", "Grade", "programme name") and vi represents the corresponding value (e.g., "Database", "A", "NLP").

Step 2: Named Entity Recognition (NER)

Using NER, we extract entities from D .

$$E = \{e1, e2, \dots, en\}$$

Where E is the set of extracted entities.

Step 3: Template-Based Question Generation

Define a set of question templates T where each template T_j can be represented as a function of entities ei .

$$T = \{T1, T2, \dots, Tm\}$$

Each template T_j is a function that takes one or more entities as input and outputs a question. For example:

$$T1(ei) = \text{"What grade did you receive in " + } ei \text{ + "?"}$$

Step 4: Selecting Entities and Generating Questions

For each entity $ei \in E$, select an appropriate template T_j and generate a question Qk .

$$Qk = T_j(ei)$$

The set of generated questions Q can be represented as:

$$Q = \{Q1, Q2, \dots, Qp\}$$

Where each Qk is a question generated by applying a template to an entity.

Step 5: Answer Extraction

For each generated question Qk , extract the corresponding answer Ak from the dataset D.

Let A be the set of answers:

$$A = \{A1, A2, \dots, Ap\}$$

where each Ak corresponds to the correct answer for question Qk .

Step 6: Mathematical Representation of the Process

i. Data Extraction:

$$E = \text{NER}(D)$$

ii. Template-Based Question Generation:

For each entity $ei \in E$:

$$Q_k = T_j(ei)$$

ii. Answer Extraction:

For each generated question Q_k :

$$A_k = D(ei)$$

Example Workflow

Consider a simplified dataset D of the developed NLP model:

$$D = \{ ("Course Name", "Database"), ("Grade", "A"), ("Programme name", "BD.HRM") \}$$

Extract entities:

$$E = \{ "Databse", "A", "Database", "BD.HRM" \}$$

4.5.5.3 System Describing the Working Mechanism of the Enhanced NLP Model

The improved impersonation detection Model was implanted in different frameworks to form a system. In this regard, the generation of dynamic challenging questions is activated by a successful scan of a QR code scanned by a mobile phone scanner connected to a mobile application. Information for generating dynamic challenging questions are extracted from a student's profile database which include student's admission information, examinations records, course details, course facilitators' details and parents of guardians details. These information are used to extend and

refine individual student's profile. Dynamic challenging questions are created in such a way that they don't cause students to feel uncomfortable by asking questions based on student's own profile in the background during students' interaction with the mechanism. In real application domain, the proposed improved impersonation detection mechanism is an actual implementation of a system that integrates all mechanism modules.

For the student to access an examination venue or room he or she must answer four (4) dynamic challenging questions that are created randomly and presented to student via mobile application interface under the supervision of the invigilator (see appendix 4). It is the role of the invigilator to confirm answers presented by a student after comparing them with the actual responses shown by the system. A successful response is recorded to the student's attendance module as a true attendance of students in that particular examination. Conversely all confirmed impersonations are reported to the examinations officer who prepares a detailed report and submit it to the office of ARC which is responsible for taking action towards an impersonations fraud. In the same line a security office is alarmed or notified of the occurrence of impersonations in the specific examination venue for them to take care of security matters see appendix for the generated Short Message Service by the system).

This study suggests a fixed number of 4 profile based dynamic challenging questions to remove the possibilities of guessing attacks as discussed later in the mechanism evaluation section. This implies that when a student appeals to access traditional examination venue, the system will automatically generates 4 dynamic challenging questions. These questions are used to verify student identity and detect

impersonations in case respondent fails to supply correct answers. In addition, the system can immediately report an impersonations in case the scanned QR code is not valid.

Therefore, an improved Mechanism for detecting impersonations is a system or an application divided into seven (7) major modules including Registration module, QR code scanning module, a module for generating DCQNS, impersonations detection module, impersonations reporting module, communication module and students' attendance taking module and . The details of the overall system components are described in Figure 4.6 through Figure 4.10.

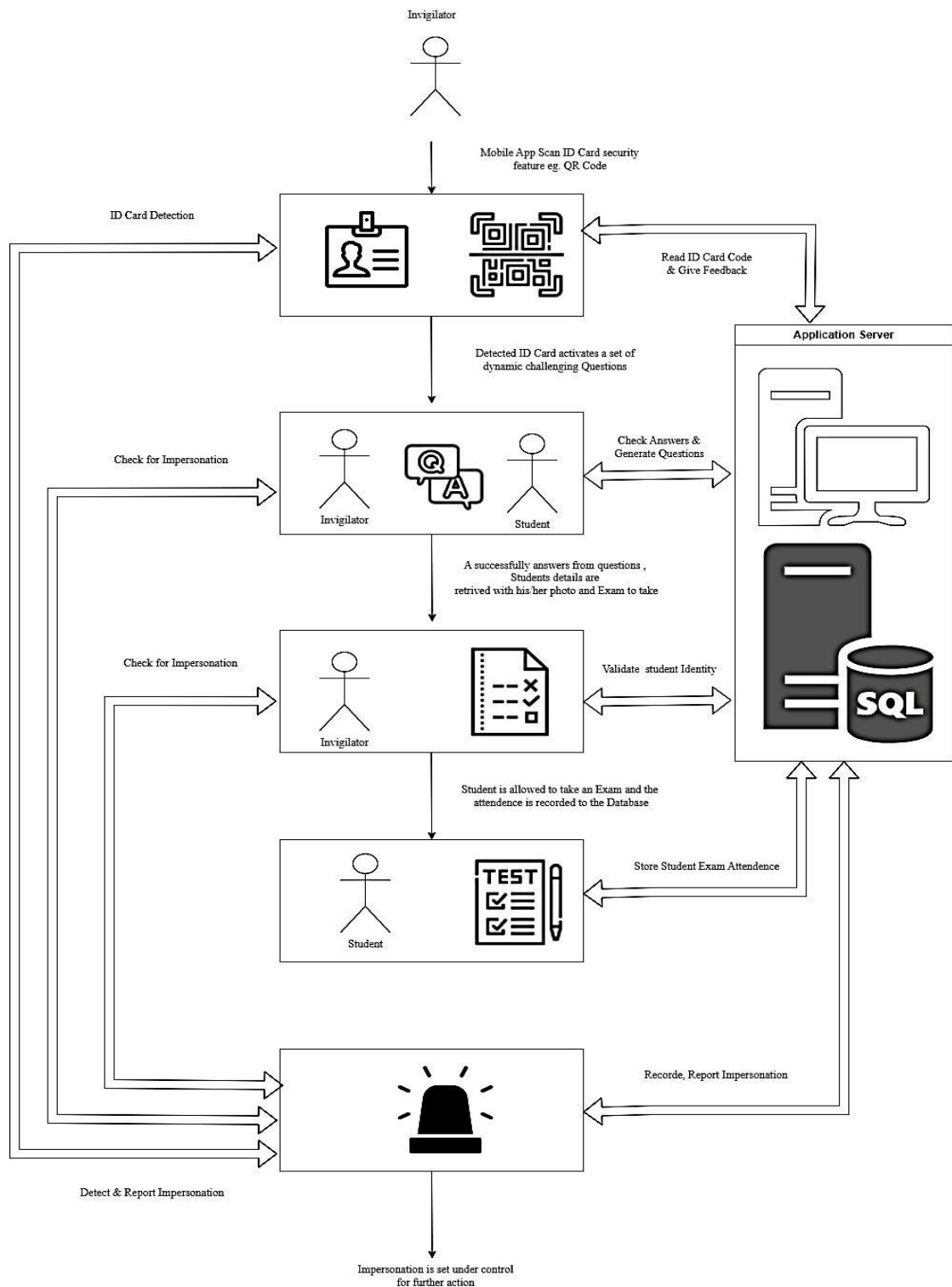


Figure 4.7: A Conceptual Design Showing how to Use the Proposed Impersonation Detection system

4.5.5.4 Use Case Diagram of the Proposed Improved Impersonations Detection System

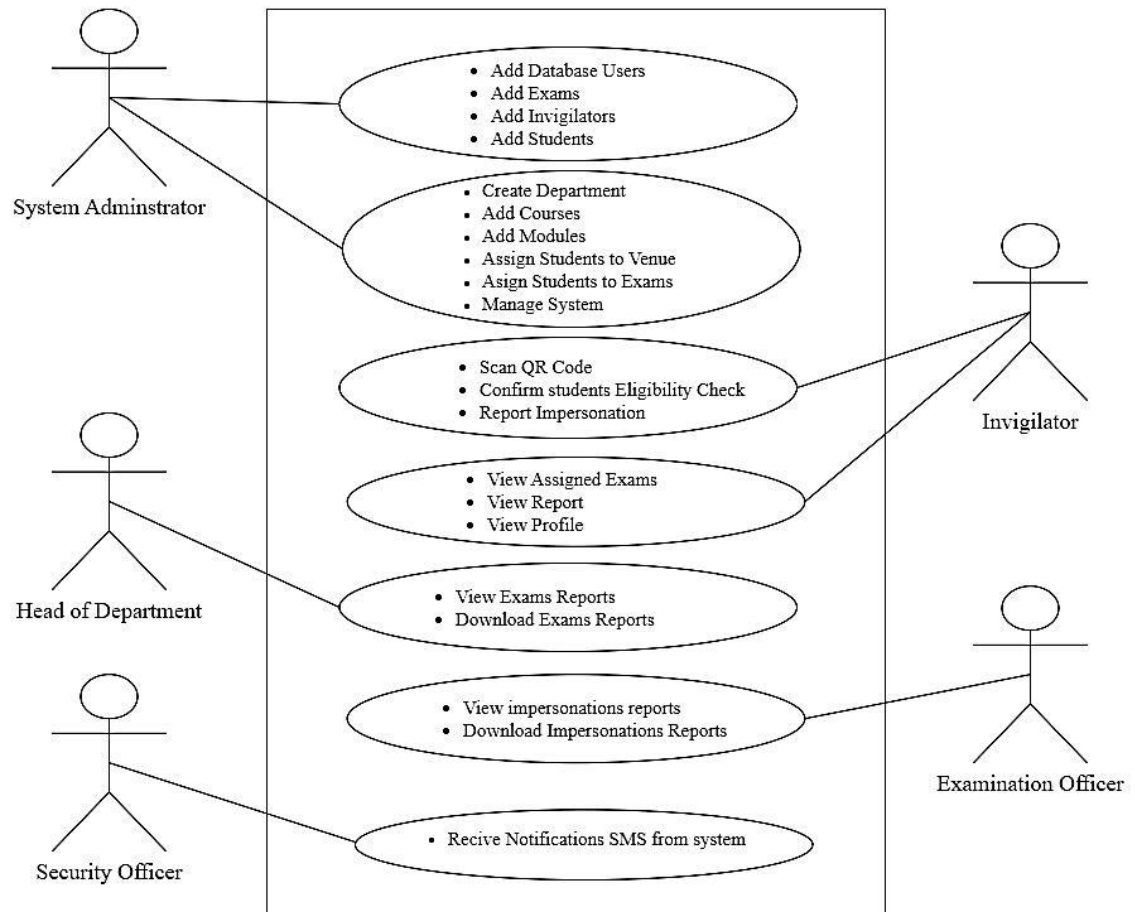


Figure 4.8: Use-Case Diagram of the Proposed System for Detecting Impersonations in Traditional-in-Class Examinations in THLIS

Source: UML

4.5.5.5 Database Design of the Proposed Impersonations Detection System

The diagram in Figure 4.9 describe a database model of the implemented improved mechanism for detecting traditional-in-class examinations impersonations. It describes an entity relationship models describing relationship between system entities.

ENTITY RELATIONSHIP DIAGRAM

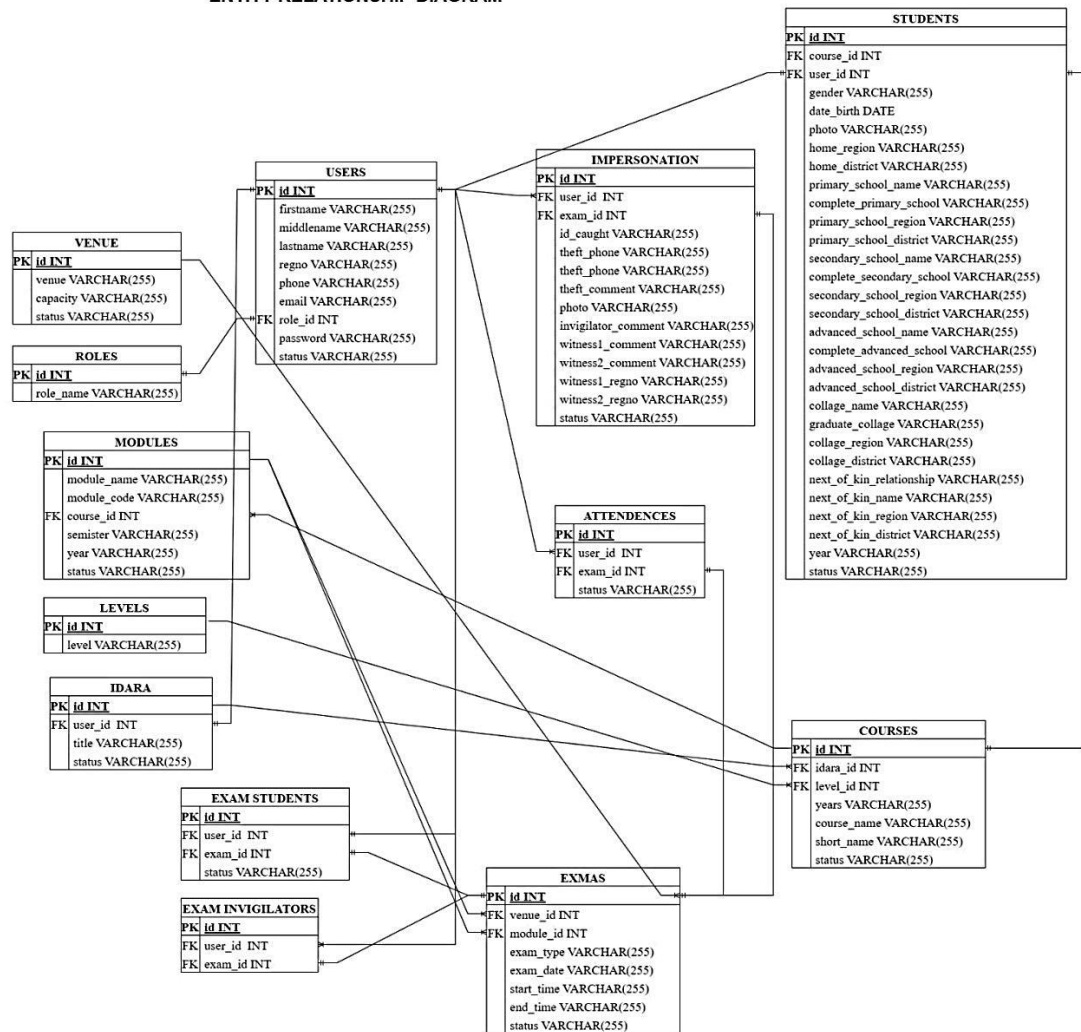


Figure 4.9: Entity Relationship Diagram (ERD-models) of the Proposed System

Source: UML

4.5.5.6 Sequence Diagram of the Proposed Improved Impersonations Detection System

The following sequence diagram in Figure 4.10 demonstrate a scenario when the student present fake identity card with invalid QR CODE. The system fails to detect it and direct operation to the impersonation detector which performs all the processes necessary to generate impersonation report.

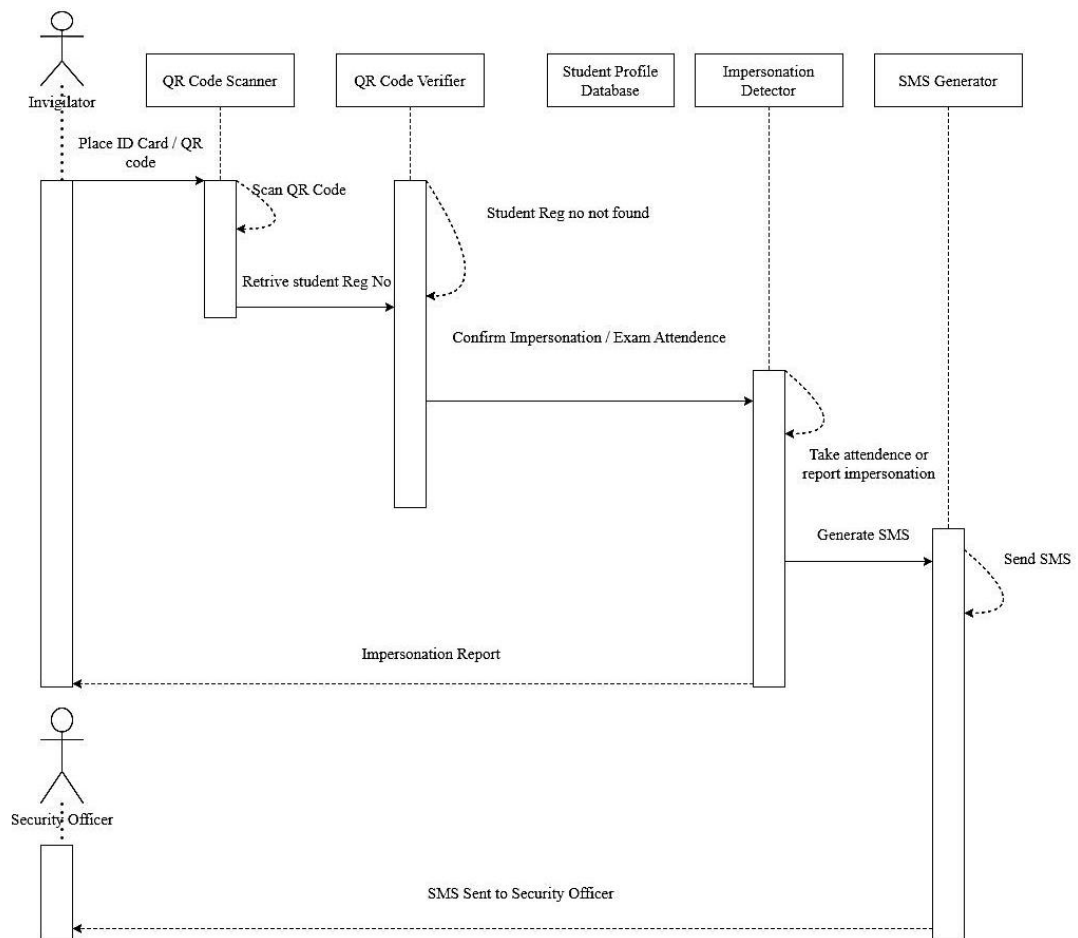


Figure 4.10: A Sequence Diagram in the Event of Fake Identity Fard/QR Code and Impersonations Detection

Source: UML

Moreover, another scenario presented by Figure 4.11 is when an impersonator presents valid identity card with valid QR Code, this scenario cause the system to subject student to a set of the dynamic challenging questions and requires a student to respond to such system questions. When an impersonator fails to supply correct responses a system is directed to an impersonation detector which performs all operations necessary to report impersonations to relevant party. In all cases an SMS generator must be activated to take necessary action for producing and sending a message call to the security officer. In the contrary if the presented QR code is

correct and a student is the original one the system proceeds with retrieving student registration number, maps it to student profile and generate a set of dynamic challenging questions and their corresponding answers, a student is required to provide questions corresponding answers, the success action leads to confirming students exam eligibility and an attendance is confirmed by an invigilators and recorded into the system database for future access by relevant institute syndicates.

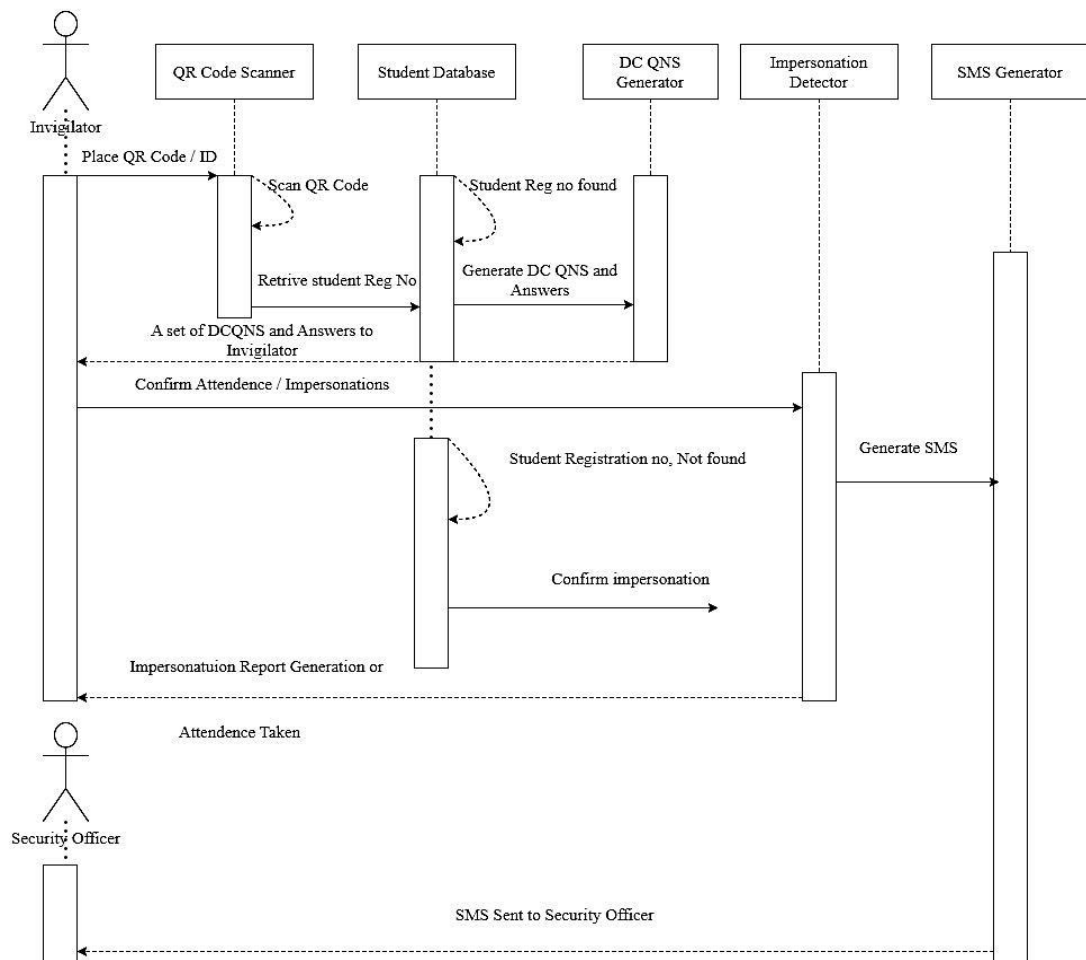


Figure 4.11: A Sequence Diagram in the Event of Presenting Valid Identity Card/QR Code but the Impersonator Fails or Pass the DCQBSP Leading to Impersonation Detection or Attendance Taking

Source: UML

4.5.6 Description of the Main Operations Presented in Figure 4.7

The diagram in Figure 4.7 describes a conceptual diagram of an improved mechanism for detecting impersonations in the context of traditional classroom examinations. The main operations the system can perform are registration or creation of student's profile commonly known as the enrollment phase, registration of examinations, registration of invigilators and verification of student's (checking student's eligibility to take an examination). During registration phase, student's profile information are captured and stored in the MYSQL database management system. Moreover, the invigilators details and examinations information including examinations venue, time and date are also captured and stored in the MYSQL database system. The first part is the interface between student and the system; a QR coded embedded in student's identity document contains student's registration number which is unique to every student. QR code are captured by the application or system through a mobile supported camera as seen in Figure 4.10. A mobile-based scanner was chosen due to its frequent employment in many mobile applications based on several reasons including the following:

Convenience: Mobile-based scanners allow users to scan documents, barcodes, QR codes, and other items directly from their mobile devices, eliminating the need for dedicated scanning hardware;

Portability: Mobile scanners enable users to carry out scanning tasks on the go, providing flexibility and convenience, especially in situations where access to traditional scanners is limited;

Integration: Mobile scanners can seamlessly integrate with various mobile applications, enabling users to scan and directly import scanned data into other apps such as the proposed mechanism for detecting impersonations in traditional-in-class examinations;

Cost-effectiveness: Mobile-based scanning solutions are often more cost-effective compared to traditional scanning equipment. Users can leverage the scanning capabilities of their existing smartphones or tablets without having to invest in additional hardware.

Efficiency: Mobile scanners can streamline workflow processes by allowing users to quickly capture and digitize documents or information, leading to increased efficiency and productivity.

Accessibility: With the widespread use of smartphones, mobile-based scanners offer accessibility to a broad range of users, making scanning functionalities readily available to individuals and businesses alike; and

Innovation: Mobile-based scanning applications continually evolve with advancements in mobile technology, offering innovative features such as optical character recognition (OCR), cloud integration, and augmented reality-based scanning, enhancing the overall scanning experience.

Equally, using mobile phone to install and use the developed application was supported by respondents where 118 (90.8%) of the respondents stated that they are

comfortable at using mobile phones and they own their own mobile phones. Figure 4.12 describes respondents' views on mobile device user friendliness as details follow in Figure 4.12

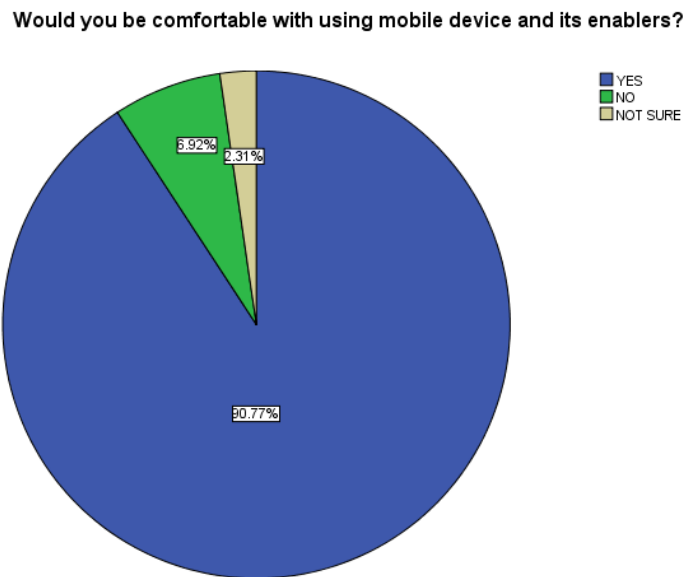


Figure 4.12: Respondent's Views on Mobile Phone User Friendliness

Overall, the use of mobile-based scanners in various mobile applications provides users with convenience, portability, cost-effectiveness, efficiency, accessibility, and continuous innovation, making them a popular choice for scanning tasks in today's digital age (Permana et al., 2021).

The second part of the system performs all the necessary pre-processing: it has to extract student's registration number from the QR code and compare it with the registration numbers stored in the students' registration database. Once the registration number is found it is linked to corresponding student's profile stored in the database.

The third part of the system involves creating a series of dynamic challenging questions based on student's profile and displaying them to the mobile screen along with their corresponding answers (see appendix 5 (d)). An invigilator utilizes the generated questions to interrogate exam candidates (students). A successful responses from a student makes an invigilator to confirm student eligibility to take a particular examination and any failure to respond to DCQNs proves an impersonations incidence to an invigilator.

The fourth part of the system involve recording attendance of all eligible candidates or report impersonations of all detected impersonations (see appendix 5 (e and f)).

The fifth part of the system involves reporting an impersonations cases to the respective unit particularly a security office letting it get informed on the occurrence of impersonations in a specific examination venue so that it can take care of security breaches in that particular examination venue (see appendix 5 (f)).

Finally all reported impersonations and attendances are made accessible to relevant offices. For the purpose of this study an examinations office can access impersonations report while head of departments can access examinations attendance sheets.

4.5.7 Designing Impersonation Detection System Based on NLP Model

The architectural design of the proposed improved mechanism for detecting impersonations in traditional-in-class examinations as shown in Figure 4.13 consists of five main blocks: the user interface, registration module, system database,

authentication module, and impersonations detection module. The user interface provides a mechanisms for a user to indicate his/her identity and input his/her QR code into the system. The system database consists of a collection of records each of which corresponds to an authorized person that has access to the system. Each record contains a profile of students' information such as students name, data of birth, school information, college information, address and next of kin information. The authentication module performs all required student verification processes and produce results that is taken to the impersonation reporting block. The impersonation reporting block performs all functions related to impersonations detection or exam eligibility check and reports impersonations to relevant authorities, takes students attendance and generate SMS necessary for notifying security officers on the incidence of impersonations.

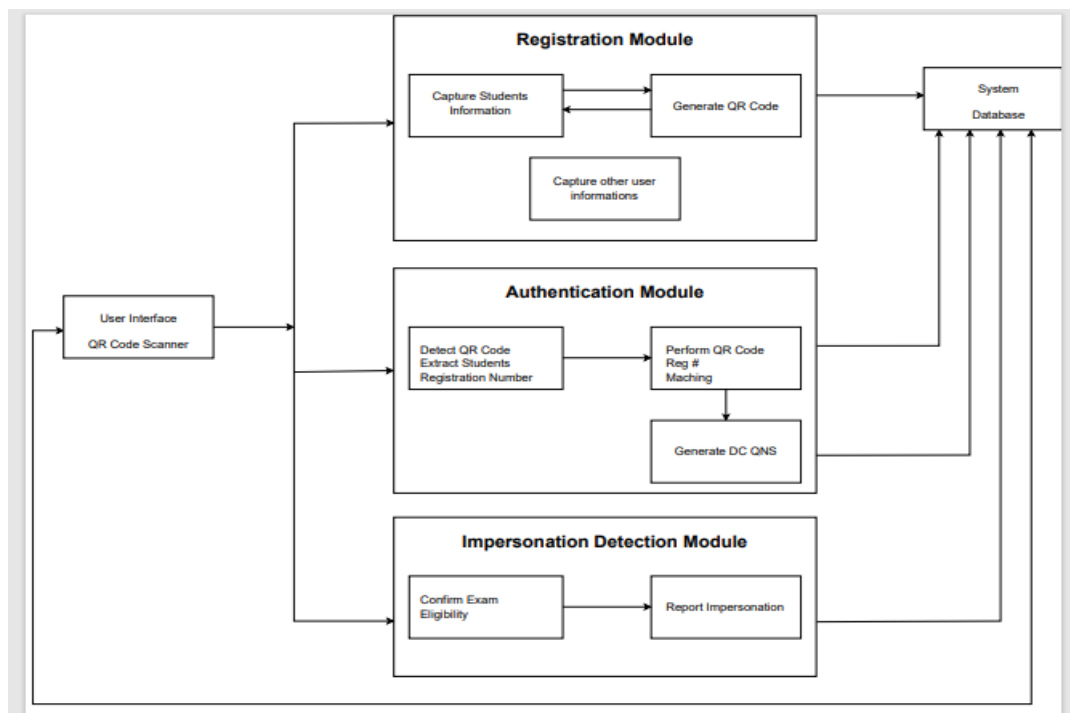


Figure 4.13: Architecture Design of the System

4.5.8 Selected Frameworks for the Implementation of the Proposed NLP Model for Detecting Impersonations in Traditional-In-Class Examinations (system)

The proposed system for detecting impersonations in traditional-in-class examinations was implemented with as an integration of Mobile Application and Web application through application interfaces (APIs). The Mobile Application was developed within a Flutter Framework together with the application interfaces (APIs) made up of restful development tools that communicate with application's backend (the server) while the Web application was implemented within the Laravel Framework that shields the hypertext Preprocessor (PHP) and a combinations of other client side markup languages such as Hypertext Markup language (HTML), Cascading Style Sheet (CSS) and scripting language including java script (JS). The database part of the application was implemented in MySQL Database management system due to various reasons including the fact that: MySQL is an open source software, which means it's freely available for use, modification, and distribution. This makes it cost-effective for businesses and developers; MySQL can handle large amounts of data and can be scaled to support growing applications and clustering options for scalability; MySQL is known for its high performance, especially when optimized properly. It can efficiently execute complex queries and handle concurrent transactions; Also MySQL is compatible with various operating systems such as Linux, Windows, macOS, and different programming languages like PHP, Python, Java, and all related languages. This compatibility makes it versatile for different application development needs.

Moreover, MySQL has a large and active community of developers and users who contribute to its development, provide support, and share resources like tutorials, forums, and plugins (Community Support); .Again, MySQL offers robust security features such as encryption, access controls, and authentication mechanisms to protect data from unauthorized access and ensure data integrity; and MySQL is a mature and stable database system that has been used in production environments for many years. It undergoes regular updates and improvements to enhance its reliability and performance (Reliability). Overall, MySQL is a powerful and versatile database solution suitable for a wide range of applications, from small websites to large enterprise systems (Domantas, 2024).

4.5.8.1 Implementation of the Mobile Application Client Side

The Application client side was implemented within Flutter Framework due to the fact that Flutter is a popular open-source UI software development kit created by Google. It's primarily used for building natively compiled applications for mobile, web, and desktop from a single codebase. It equally offers crucial features for implementing client-side applications, these features include: Single Codebase, Multiple Platforms, that is, with Flutter, developers can write code once and deploy it across multiple platforms, including iOS, Android, web, and desktop. This saves time and effort compared to developing separate codebases for each platform; flutter offers a hot reload feature, allowing developers to see the changes they make to the code almost instantly reflected in the app.

This accelerated the development process and enabled quick iteration (ie. Fast Development); Beautiful UIs: Flutter provides a rich set of customizable widgets and tools to create visually stunning and highly responsive user interfaces as seen in the snapshot included in the appendices section. Its flexible design allowed for pixel-perfect customization and smooth animations; also Performance, Flutter applications are compiled directly to native machine code, this resulted in high performance and faster startup times. Flutter more, flutter utilizes Skia, a powerful graphics engine, to render UI components, ensuring smooth performance across different devices; also flutter offers plugins and platform channels that enabled developer to access native platform features and APIs seamlessly. This allowed for deeper integration with device functionalities like camera, GPS, sensors, and more (ie. Access to Native Features); in addition, flutter has a rapidly growing community of developers, contributors, and enthusiasts who actively contribute to its development, share resources, and provide support (Growing Community and Ecosystem); Additionally, Flutter has a rich ecosystem of packages, plugins, and tools that enhance productivity and extend functionality; Flutter is an open-source framework released under the BSD license, making it free to use and distribute. This lowers the barrier to entry for developer and business, particularly startups and small teams (ie. Open Source and Free); Also Flutter is backed by Google, which provides ongoing support, updates, and improvements to the framework. This ensures the long-term stability and viability of Flutter for building production-quality applications (Official Support from Google). Flutter supports Dart Programming Language that provide features like ahead-of-time (AOT) compilation and just-in-time (JIT) compilation for efficient application development; Flutter provides

widgets and designs following Material Design for Android apps and Cupertino for iOS apps, ensuring platform-specific UI elements (Material Design (for Android) and Cupertino (for iOS)); Again, Flutter apps interact with the server-side through RESTful APIs, enabling data exchange between the client and the server. The APIs were written in Laravel code base and consumed to the app with secured baretokens on passing the data from server to the app to ensure that users using the data are authenticated users only (Integration with RESTful APIs).

4.5.8.2 Implementation of the Web Server Side

The Web side was implemented in Laravel Framework. The Laravel is a PHP web application framework known for its elegant syntax and modular packaging. Laravel Framework follows the Model-View-Controller (MVC) architectural pattern, which provides a clear separation of concerns and helps organize code in a structured manner. This made it easier to manage and maintain web applications, especially as they grow in complexity (Robust MVC Architecture); also Laravel has expressive syntax which provided an expressive and elegant syntax that simplified common tasks such as routing, authentication, caching, and database operations. This allowed the developer to write clean and concise code, improving readability and productivity; In addition, a Laravel has a rich feature set which comes with a wide range of built-in features and functionalities, including database migrations, Eloquent ORM (Object-Relational Mapping), form validation, queueing, task scheduling, and more. These features helped the developer to build powerful and feature-rich web application quickly and efficiently, more over; Laravel has a large and active community of developers who contribute to its development, share knowledge, and

provide support through forums, tutorials, and packages a feature commonly known as Community Support. This community-driven ecosystem ensures that developers have access to resources and solutions to common problems; furthermore, Laravel prioritizes security and includes built-in features this developer protect student verification applications from common security threats such as SQL injection, cross-site request forgery (CSRF), and cross-site scripting (XSS) attacks (Security);

Additionally, Laravel's authentication and authorization mechanisms made it easy to implement secure user authentication and access control; Laravel supports multiple database systems out of the box, including MySQL, PostgreSQL, SQLite, and SQL Server (Database Agnostic). This flexibility allowed the developer to choose the database that best suits this project requirements without being tied to a specific vendor particularly the MySQL which is supported by PhPMyadmin database tool to create, manipulate and manage the Database objects and assist the migrations from Laravel commands; Laravel includes the Blade templating engine, which provides a simple yet powerful way to create reusable and dynamic views. Blade templates allowed developer to write clean and concise HTML codes mixed with PHP logics, making it easier to manage the presentation layer of web applications (Blade Templating Engine); and Laravel offers seamless integration with popular third-party services and APIs through Composer packages and Laravel-specific libraries. This enabled developer to extend the functionality of student verification application by integrating with services such as SMS gateway and cloud storage (Setiawana, Suharjito and Diana, 2019) and (Richard, 2022).

Overall, Laravel provided developer with a robust and feature-rich framework for building web server-side student verification application, making it a popular choice for both small-scale projects and large-scale enterprise applications.

4.5.8.3 Generation of QR codes

To facilitate the generation of QR code used by the client student verification application to authenticate students the system includes a mechanism to generate QR codes using the Laravel package known as "milon/barcode". This package simplifies the process of generating QR codes within Laravel applications, enhancing the system's functionality for QR code-based interactions. The package is managed and supported securely by Laravel composer organization. The "milon/barcode" package for Laravel users allows application administrator to generate various types of barcodes, including QR codes. Here's a basic overview of how package was used to generate QR codes within a Laravel application:

The first step was to install the "milon/barcode" package via Composer through running the following command in the developed Laravel project directory: “composer require milon/barcode”; secondly, after installing the package, it was used to generate QR codes in the developed Laravel application know as student authentication system (SAS). Figure 4.14 present codes used to generate a QR.

```
// Generate QR code with student data (Registration number)

<span class="text-danger"> {!! DNS2D::getBarcodeHTML($student->user->regno,
'QRCODE', 10, 10) !!}</span>
```

Figure 4.14: Generate QR Code with Student Data (Registration number)

The code generates a QR code image containing student's registration number. Once a QR code has been generated it is displayed in a Laravel application using relevant codes. Again, the "milon/barcode" package allows to customize various aspects of the generated QR codes, such as size, color, error correction level, and format.

Generally, the "milon/barcode" package provides a convenient way to generate QR codes within a Laravel application, allowing developer to easily integrate QR code generation functionality into an improved mechanism for detecting impersonations in the context of traditional in-class examinations in Tanzania public higher learning institutions.

4.5.8.4 Summary

The web and mobile application system developed by using Laravel and Flutter leverages modern technologies to provide a seamless user experience across different platforms. With Flutter handling the client-side development and Laravel powering the server-side logic, the system ensures efficiency, scalability, and maintainability. Additionally, the integration of QR code generation using "milon/barcode" enhances

the system's capabilities, enabling various use cases involving QR code-based interactions.

4.5.9 The Actual Implementation of Core Parts of the Proposed Impersonations Detection System (Coding)

This section entails an actual implementation of core parts of the system. This effort produced a live mobile application that facilitate an evaluation of the proposed NLP model.

4.5.9.1 Codes for Scanning Student' QR code

QR code is scanned on the client application connected to the mobile scanner. The QR codes contains student's registration number which is connected to students' profile in the database system (see appendix 6 (a)).

4.5.9.2 Generating Dynamic Challenging Questions (DCQNs) based on Student Profile

For each valid QR code, a next step for generating DCQNs is triggered to generate the DCQNs that is based on student profile. The questions are generated along with their corresponding answers that are displayed on the user interface (the mobile screen) held by the invigilator. It will depend on the matching of answers between those generated by the system and those produced by the student before an invigilator can confirm student's eligibility for that examination through the system. An incorrect answers will be accounted for an impersonations case while for all correct answers are accounted as eligible candidate. The mechanism in appendix 6

(b) describes an implementation that generate DCQNs based on student profile along with their corresponding answers.

4.5.9.3 Confirming Students Attendance

The implementation in appendix 6(c) describes the mechanism of student's attendance confirmation.

4.5.9.4 Confirming and Reporting Impersonations

The mechanism in appendixes 6 (d) describe the implementation for reporting impersonations and taking students' attendance.

4.5.9.5 Implementing user Login Page (Administrator Page and other System Users) on the Web Application

The codes in appendix 6 (e) demonstrate the implementation of user login page in the client side on the web side of the application.

4.5.9.6 Implementing user Login Page (Administrator Page and other Susers) on the Mobile Application (Invigilator Only)

The codes in appendix 6 (f) describe the implementation of the user login Page (Administrator page and other system users) on the Mobile Application.

4.5.9.7 Adding New Examination to the Database

The mechanism for creating new examination to the database is described in the

implementation of the module for adding examinations in the impersonations detection database (see appendix 6 (g)).]

4.5.9.8 Assigning Students to an Examination

The mechanism for assigning students to examination is demonstrated in appendix 6 (h) which shows the implementation a module for adding students to examination (examination registration).

4.5.9.9 Adding Students to the Database (Students Registration)

The implementation in appendix 6 (i) demonstrates the implementation of a module for registering students (students' registration).

4.5.9.10 Adding Invigilators to the Database (Invigilators Registration)

The mechanism in 6 (j) demonstrate the implementation of a module for registering invigilators who are responsible for monitoring the student authentication application (invigilators registration).

4.5.10 The Major User Interfaces from the Proposed Improved Impersonations Detection System

The selected User Interfaces from the proposed Improved Impersonations Detection Mechanism showcase a significant advancement in impersonations detection technologies in traditional classroom examinations particularly in Tanzania public higher learning institutions which have been designed to bolster impersonations detection measures in same context, these interfaces represent a culmination of

innovative techniques aimed at detecting and preventing impersonations. By leveraging state-of-the-art algorithms and intuitive design principles, these interfaces promise to provide users with robust protection against malicious actors attempting to impersonate legitimate entities. Through this groundbreaking mechanism, users can use the system platform with confidence, knowing that they can precisely detect impersonations cases. Figure 4.15 represent a sample system interface where, rest of the system's user interfaces are presented in appendix 5 (a) through 5 (f) of this report.

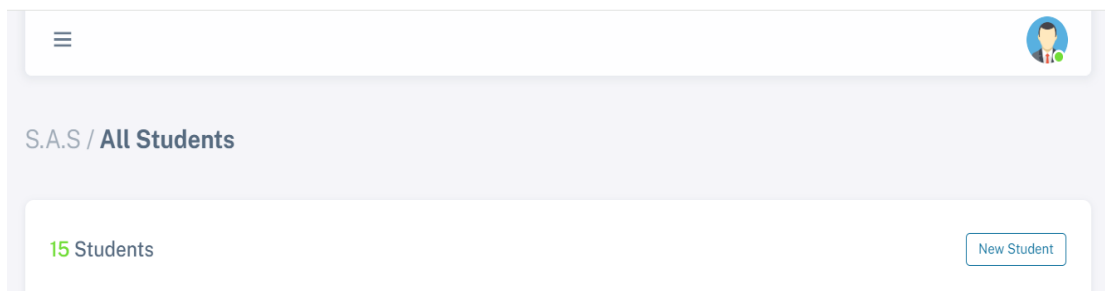


Figure 4.15: A Students Registration Interface

4.6 Evaluating the Proposed Improved Impersonations Detection Model

This section presents findings and discussion driven from the data collected and analyzed to achieve specific objective three (3) which intended to evaluate the proposed improved impersonations detection mechanism for traditional-in-class examinations. This rest of the section is organized into section 4.6.1 which describes student registration component, section 4.6.2 presents results from the usability test, section 4.6.3 describes the efficiency of generating dynamic challenging questions

based on students' profile along with their corresponding answers and section 4.6.4 describes performing a response time acceptance testing. In addition section 4.6.5 performs some analysis to test the mechanism reliability accuracy.

4.6.1 Students Registration

In order to test functionalities of the proposed mechanism, fifty (50) students were enrolled into the system and registered for various examinations, these examinations include semester examinations, supplantentay examinations, special examinations, and tests. The majority 40 (80%) were third year students perusing bachelor degree in education and 10 (20%) students were pursuing Ordinary Diploma in Economics Development due to their experiences in higher education learning. Also these students were promised a lump sum of TShs. 100 000/= if they could successfully simulate their colleagues profiles and attempt to deceive the system (execute impersonations). This was done to encourage students perform the security abuse case scenarios. However, the participation was voluntary and performed with real students in order to create real examinations context. This led to a smaller sample size as discussed in a later section.

The researcher intended to establish the efficiency of the proposed improved mechanism for detecting impersonations and whether a student could share their profile information with third party impersonators before coming to the examination room (venue) and successfully execute impersonations. To successfully achieve this objective a usability test approach was used to assess the efficiency of the

mechanism while a false rejection and false acceptance parameters were employed to assess the mechanism reliability and accuracy.

4.6.2 Usability Assessment of the Proposed Impersonation Detection Mechanism

Corry, Frick, and Hansen (1977) presents that a usability assessment is emphasized on human computer interaction (HCI). In this regards, fifty (50) valid students were identified through the developed impersonations detection mechanism (system) which integrates QR codes embedded on student cards and dynamic challenging questions based on students' profiles. Also 50 students (impersonators) were recruited to attempt impersonate their fellow students and each impersonator was allowed to simulate his or her colleagues profile information five (5) days before an actual date of performing a usability assessment of the system. Five (5) days were determined enough for impersonators to simulate profile information of their colleagues. Several manipulations was performed using abuse case scenarios to test and assess impersonations attacks on the proposed mechanism. The abuse case scenarios were adopted to check impersonations attacks when students were allowed to exchange their personal profile information. To complete this assessment, 50 impersonators were asked to respond to for (4) dynamic challenging questions that were associated with other students. Results from usability test were recorded as shown in Table 4.8 and Table 4.9.

Table 4.8: Results from Authenticating and Verifying Gstudents.

Number of Test Case (NTC) (Abuse case scenarios)	Number of DCQS Generated by the system	Number of correct response generated by the system	Number of Correct Responses given by genuine students	Percentage of Correct Responses given by genuine students (%)	Number of Incorrect Responses given by genuine students	Percentage of Incorrect Responses from the impersonators (%)
50	200	200	200	100	0	0

Source; Field Data, 2024

Table 4.9: Impersonators Responses and Percentages of Correct Answers

During Authentication and Verification of their Identities

Number of 1 Correct Response given by impersonators <=1	Percent age	Number of 2 Correct Responses given by impersonators	Percent age	Number of 3 Correct Responses given by impersonators	Percent age	Number of 4 Correct Responses given by impersonators	Percent age
40	80	5	10	4	8	1	2

4.6.2.1 Results from System' Usability Assessment

This section presents findings from usability test of dynamic challenging questions based on student profile in the context of traditional-in-class examinations. A total of 50 impersonators responded to 200 challenging questions generated by the system for their identification and examination eligibility check. The time taken to generate four (4) challenging questions was approximately one (1) second, students' responses varied depending on individual student cognitive abilities and system operator speed. Attendance was captured after each successful student identification (see appendix 5.14 for student attendance sheet snapshot). The output shows that students'

identification efficiency was improved compared to the current identity cards based students identifications. Also the system was able to detect impersonators who came with fake QR code and those who had valid QR code but failed to respond to challenging questions generated by the system. Efficiency analysis is presented in the next section.

4.6.3 Efficiency of Generating Dynamic Challenging Questions Based on Students' Profile Along with their Corresponding Answers

In the context of this study, the efficiency is considered to be the degree of accuracy of the system to generate dynamic challenging questions based on student profile, their correct corresponding answers and students' responses with a low error rate. This was analyzed from the data collected from challenging questions and their corresponding answers generated by the system. Table 4.8 and table 4.9 has shown the analysis of dynamic challenging questions and the percentage of correct answers. The results show that the system was able to generate dynamic challenging questions based on students' profile along with their correct answers. Again, it shows that, large number of answers given by impersonators (80%) were incorrect. Out of 200 questions generated from a system only 40 (20%) impersonators' responses or answers were correct and 160 (80%) responses or answers given by impersonators were incorrect. In the other hand only 40 (80%) impersonators could produce at most 1 correct answer among the four (4) asked challenging questions while 5 (10%) impersonators could provide 2 correct answers among the 4 asked questions, 4 impersonators could provide 3 correct answers while only 1 (2%) could completely deceive the system. This implies that to prevent guessing attack or correct answers

by chance number of challenging questions could be increased by at least 4 questions. Again Table 4.10 shows the sample dynamic challenging questions generated by the system. This results show satisfactory system or mechanism efficiency since the system could produce 200 dynamic challenging questions containing different categories of profile information, this implies that it is difficult for a student to share questions and answers which account for low impersonations attack. Also the mechanism demonstrated great accuracy in generating dynamic challenging questions in a random fashion making it difficult for the impersonators to predict the questions generation mechanism. Sample dynamic challenging questions generated by the system are included in appendix 4.

Moreover, participants were asked to mention correct answers and the invigilator could display the correct answers on the screen and compare them with student responses. Results indicate that 98% of Impersonators' could not respond to all four (4) questions (Table 4.9). The mechanism was able to produce questions and their correct answers which is quite impossible for an invigilator to do as it would take them a couple of years to internalize student's' profile information. Bangor, Kortum and Miller (2009) described a usability scale which states that 70% to 79% are acceptable, 80% to 89% are good, and more than 90% is exceptional. Thus, generating 100% correct dynamic challenging questions along their corresponding answers from the system is an exceptional performance and therefore, an improved mechanism for generating dynamic challenging questions is very effective. In a nutshell, these results implies that an algorithm utilizes different student information to generate questions that make it difficult for the impersonators to predict kind of

profile question that will be generated from a system hence difficult for them to attack the system.

Table 4.10: Analysis of the Efficiency of Generating Dynamic Challenging Questions Based on Student Profile

S/N	Questions Category	Correct Question	Corresponding Correct Answers
1	Questions on students particulars	63 (31.5%)	63 (100%)
3	Questions on School Background Information	71 (35.5%)	71 (100%)
4	Questions on parents/guardians details	36 (18%)	36 (100%)
5	Questions on University information	30 (15%)	30(100%)

4.6.4 Performing a Response Time Acceptance Testing

Several studies indicate that response time to dynamic challenging questions generation should be small since questions should be created un-intrusively an un-distractingly in the system. This is well demonstrated by the proposed improved mechanism for detecting impersonations as it takes at most 2 seconds to generate 4 different dynamic challenging questions (see Table 4.10). This approach indicates that there is an increased response time when compared to current ID based identification system which takes at least 1 minute to effectively identify one student (Xiao, Barke, 2108). On the other hand, the study revealed that the likelihood of guessing the correct answer is 80% if dynamic question was 1. Consequently, to prevent correct answers through guessing, a student should be presented with at least four (4) dynamic challenging questions. This evidence is shown in table 4.9 above. Also results show that one invigilator can verify 200 students in almost 33 minutes.

This time is an average time stated in examination guidelines and procedures of the academy for it requires students and invigilators to arrive at the examination venue 30 minutes before commencement of an examination (MNMA Examinations Guidelines and Procedures, 2024). This means that if an examination venue has three invigilators almost 11 minutes are enough for them to verify students' examination's eligibility with great accuracy.

Moreover, to ensure the stability and performance of the proposed impersonation detection system under large-scale use the following strategies were implemented:

Scalable Infrastructure: the system was deployed in Play Store cloud platform that supports auto-scaling. This allows the system to handle varying loads by automatically adjusting resources based on demand.

Efficient Database Management: The MySQL database was optimized for performance by using indexing, query optimization, and proper schema design. Caching mechanisms was employed to reduce database load for frequently accessed data.

Load Balancing: the deployment platform use load balancers to distribute incoming traffic evenly across multiple servers. This ensures no single server becomes a bottleneck and enhances overall system performance.

Robust API Design: The RESTful APIs used for communication between the mobile ap-plication and backend are efficient and well-optimized. Rate limiting was

implemented to prevent abuse and ensure the system remains responsive under high load.

Parallel Processing: the system implements parallel processing for generating dynamic questions and verifying student identities. This significantly reduce the time taken per request and improve throughput.

For future improvements it is suggested to optimize Code by regularly reviewing and op-timizing the codebase for both the mobile application and the backend system and en-sure efficient use of resources and minimize latency in processing requests.

Other considerations include:

Content Delivery Network (CDN): Utilize a CDN to serve static content and reduce load on the main servers. This helps improve response times for users distributed across different geographical locations.

Regular Maintenance and Updates: Keep the system updated with the latest security patches and performance improvements. Regularly perform maintenance to ensure the system remains stable and secure.

Redundancy and Failover Mechanisms: Implement redundancy for critical components and failover mechanisms to ensure continuous operation even in the event of hardware or software failures.

By incorporating these strategies, the system can maintain stability and high performance even under large-scale use, ensuring reliable and efficient verification of student identities.

4.6.5 Performing some Analysis to Test the System's Reliability and Accuracy

A researcher owed to establish the reliability and accuracy of the proposed system. To achieve this purpose a false rejection (FR) and false acceptance (FA) parameters were used (Akinola¹, Abayomi-Alli and Adeniyi, 2015).

4.6.5.1 False Rejection

False rejection refers to a situation where the developed mechanism fails to identify an actual student. That the mechanism identifies a valid student as an impersonator (NSTC Subcommittee on Biometrics, 2006) and (Sindha, 2012). In the context of the proposed mechanism, false rejection occurs when the mechanism generates questions that are very difficult even for the valid student. For instance, if the mechanism generates questions concerning details from the students' childhood that they can't remember, it could mistakenly reject valid student. Furthermore, however QR codes can be used as a secure means of identifying users it can result in a false rejection if there is an error in the QR code generation or scanning process. Now integrating both profile based dynamic challenging questions and QR codes identification scheme adds layers of security, but it also increases the chances of false rejection. If either component malfunctions or encounters an issue, it could result in the rejection of the valid student. To mitigate false rejection cases, it was essential to carefully design the mechanism that ensure that the questions were reasonable and relevant to

the students' profile and that the QR code authentication process is robust and reliable. The following measures were implemented to handle misidentification of QR codes and ensure IMDIs system accuracy and reliability:

QR Code Quality Control: QR codes are printed with high quality and a robust design that includes error correction was applied. This helps in maintaining readability even if the QR code is partially damaged.

Redundancy in QR Code Data: redundant data was included in the QR code to allow for error correction. QR codes have built-in error correction capabilities (L, M, Q, H levels), which was set to a higher level.

Multiple Scans and Cross-Verification: A multiple scans of the QR code if the first scan fails was enabled. Cross-verification mechanism where the system checks the scanned data against the database to confirm accuracy was also implemented.

User Feedback Mechanism: The system provides immediate feedback to the user if the QR code scan fails or if there is a misidentification. This allow users to retry the scan or manually enter their identification details if necessary.

Use of High-Quality Scanners: the IMDIs app was installed in a smart phone with high-quality QR code scanners that can read codes quickly and accurately, even under less-than-ideal conditions (e.g., poor lighting, reflective surfaces).

Backup Identification Methods: A backup methods for identification was implemented, such as using manual verification by the invigilator or entering student registration number manually.

In addition, it is recommended that there should be a Regular Updates and Maintenance, performing a Logging Analysis for system improvement and Training Users. By incorporating these measures, the system can effectively handle misidentifications of QR codes, ensuring a smooth and reliable verification process.

4.6.5.2 False Rejection Rate (FRR)

The false rejection rate accounts for the measure of the probability that the proposed impersonation detection mechanism will reject valid student and detect him or her as impersonator. The mathematical representation of this scenario is: ***FRR = Number of false rejection / Total Number of attempts***. To test for the false rejection, 50 students were registered and identified two times to check if the false rejection could occur (Table 4.11 shows the results). Results shows that there were no false rejection in the propose impersonation detection mechanism.

Table 4.11: Result of the Test Carried out on the System

Total Sample	FR	FRR (%)
50	-	-

Where, FR is the false rejection and FRR is the false rejection rate

4.6.5.3 False Acceptance (FA)

False acceptance refers to the situation where the proposed mechanism incorrectly

verifies invalid students. This phenomenon gives invalid student access to the examination venue. In the context of this research, false acceptance occurs when a mechanism generates questions that are too generic or easy to guess. This may cause an impersonator to answer questions correctly, thus gaining access to the examination venue. For instance if the challenging questions are based on publicly available information or common knowledge, an impersonator could easily gather this information and pass the identification process (Das and Debbarma, 2011) and (Anthony and Bertino, 2012).). Again, a QR code identification can be duplicated or intercepted by an impersonator. If an impersonator manages to obtain a copy of the genuine user's QR code, they could potentially use it to gain access to the system.

An integration exploit the weakness. If there are vulnerabilities in the integration between the profile dynamic challenging questions and QR code authentication components, an attacker could exploit these weaknesses to bypass the authentication process. For example, if there's a flaw in the communication between the two components or if they don't properly validate each other's responses, it could open up opportunities for false acceptance.

To prevent false acceptance scenarios, it was crucial to implement robust security measures such as: Ensuring that challenging questions are dynamic and genuinely challenging and not easily guessable or obtainable through public information, implementing additional layers of authentication using QR code, regularly updating and patching the system to address any vulnerabilities or weaknesses and monitoring

for suspicious activities or anomalies in authentication attempts and implementing measures to detect and mitigate potential attacks.

4.6.5.4 False Acceptance Rate (FAR)

False acceptance rate refers to the probability of the proposed impersonation detection mechanism to incorrectly accept the input QR code. To determine FAR, 50 students were registered and then were asked to impersonate valid students. Some impersonators used correct QR codes while others used fake QR codes. Results show that one student could be incorrectly accepted by the system hence 1 false acceptance in the proposed impersonation detection mechanism (see Table 4.12). This could be reduced by either adding number of questions or complicating student profile.

Table 4.12: Result of the Test Carried out on the System.

Total Sample	FA	FAR (%)
50	1	0.02

4.6.5.5 Convenience

Convenience formula based on false rejection scenarios was applied in an impersonation detection system utilizing profile dynamic challenging questions and QR codes to demonstrate how it is conducive to use the proposed impersonation detection mechanism. Such a formula helped strike a balance between security and user convenience by adjusting the parameters of the authentication process. Some techniques such as system adaptability, QR code reliability and feedback mechanism were employed to improve convenience.

4.6.5.5.1 Adaptive Question Difficulty

The system could adapt the difficulty of the challenging questions based on the user's past performance and feedback. If a user consistently struggles with certain types of questions, the system operator could adjust the difficulty level to make them easier by generating more questions, thus reducing the likelihood of false rejections while still providing adequate security.

4.6.5.5.2 QR code Reliability

The system could analyze the reliability of QR code scans and adjust its reliance on this authentication method accordingly. If QR code scans frequently fail or produce false rejections, the system could rely more heavily on challenging questions or other authentication methods to ensure a smoother user experience.

4.6.5.5.3 Feedback Mechanism

Implementing a feedback mechanism where users can report false rejections can also inform the system's adjustments. If a significant number of users report false rejections, the system administrator can analyze the reported cases to identify patterns and adjust its parameters accordingly to minimize future occurrences.

Generally, False Rejection Rate (FRR) was used to assess the convenience of the proposed impersonation detection mechanism. Results show that the proposed impersonation detection mechanism is convenient to the user with 1 (100%) convenience which is mathematically represented as follows (Lourde and Dushyant, 2010).

$$\textit{Convenience} = 1 - \textit{FRR}$$

Using Table 4.11 results, then

$$\textit{Convenience} = 1 - 0 = 1$$

4.6.5.5.4 Summary

By incorporating these elements into the impersonation detection system, a more user-friendly experience was created while still maintaining a high level of security against impersonation attempts. The convenience formula aims to optimize the trade-off between security and user convenience by dynamically adjusting authentication parameters based on real-time feedback and system performance.

4.6.5.6 Security

Security show the reliability and security of the proposed improved mechanism for detecting impersonations in traditional-in-class examinations. Security for this case depends on the false acceptance rate (FAR) that occurred while the system was being tested. Since the mathematical calculations presents 0.02 FAR occurred during testing the mechanism, then it imperative to state that the mechanism (system) is 98% protected and perfect (see the mathematical derivation below).

$$\textit{Security} = 1 - \textit{FAR}$$

$$\textit{Security} = 1 - 0.02 = 0.98 \text{ (98\%)}$$

$$\textit{Security} = 0.98 \text{ (98\%)}$$

4.6.6 Deployment of the Proposed IMDIs System

The IMDIs system comprises a mobile application and a web-based platform. The mobile application, developed using the Flutter Framework, scans QR codes on

student IDs, which links to dynamic profile questions generated in real-time using natural language processing (NLP) algorithms. These personalized questions are based on the student's profile and are designed to be answered correctly only by the legitimate student, enhancing security.

The web-based system, built with the Laravel Framework, manages the backend operations, including the generation of dynamic questions and communication with the database, implemented using MySQL. When a student arrives at the examination venue, the invigilator scans the QR code on the student's ID using the mobile application. The application then generates and displays a set of dynamic questions on the screen.

The student must answer these questions correctly to be verified. This process typically takes around two seconds per student, allowing the verification of a large number of students efficiently. The system logs each verification attempt, facilitating attendance tracking and providing a mechanism for real-time alerts to security officers if impersonation is detected. This deployment ensures a secure, efficient, and scalable solution for verifying student identities and preventing examination impersonations during traditional-in-class examinations such as Tests, Semester examinations and Supplementary examinations.

4.7 Significance of this Study

The development of a NLP model that generates dynamic profile questions and integrate with a QR code to verify the identity of a student holds significant

implications for various stakeholders in the educational ecosystem. The significance of this study can be outlined as follows:

4.7.1 Enhanced Security and Verification

The integration of dynamic profile questions and QR code verification enhances the security of student identity verification processes. This ensures that only authenticated students can access sensitive resources such as Library rooms and study rooms, participate in exams, and benefit from all institutional resources, reducing the risk of identity fraud.

4.7.2 Streamlined Administrative Processes

Automating the generation of profile questions and QR codes simplifies the administrative tasks related to student enrollment and verification. This can lead to more efficient operations, saving time and resources for educational institutions.

4.7.3 Improved Data Accuracy and Integrity

The use of dynamic questions ensures that the data collected is current and relevant, leading to higher accuracy and integrity of student information. This is crucial for maintaining reliable records and making informed decisions based on student data and response.

4.7.4 Increased Student Engagement and Satisfaction

When students feel confident in the security and efficiency of their educational environment, their overall engagement and satisfaction with the institution are likely

to increase. A seamless verification process can enhance the student experience, fostering a positive relationship with the institution.

4.7.5 Support for Remote and Online Learning

With the growing trend towards remote and online learning, secure and reliable identity verification becomes even more critical. This model supports these modalities by providing a robust solution that can be easily integrated into online platforms.

4.7.6 Compliance with Regulatory Standards

Educational institutions are often required to comply with various regulatory standards set by Regulators such as the National Council for Technical and Vocational Education and Training (NACTVET) and the Tanzania Commission for Universities (TCU) regarding data privacy and identity verification. This model aids in meeting these requirements, ensuring that institutions remain compliant and avoid potential legal issues.

4.7.7 Innovation in Educational Technology

This study contributes to the broader field of educational technology by introducing innovative solutions for student verification. It opens avenues for further research and development, encouraging continuous improvement and adaptation of new technologies in education.

In a nutshell, the significance of this study lies in its potential to transform student identity verification processes, leading to enhanced security, efficiency, and

personalization in education. It addresses critical challenges faced by educational institutions and aligns with the evolving needs of modern education systems.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This study was conducted to propose an improved mechanism for detecting impersonations in traditional-in-class examinations. The study has three specific objectives that have been addressed including identifying prominent technologies suitable for detecting impersonations during traditional-in-class examinations, developing an enhanced natural language processing (NLP) model which detects impersonations in the context of traditional-in-class examinations and evaluating the efficiency of the developed enhanced NLP model which detects impersonations in the context of traditional-in-class examinations. The improved mechanism for detecting impersonations in traditional-in-class examinations have been proposed. This solution is made possible by using a enhanced NLP model which is an integration of a dynamic challenging questions generation technique and QR code which act as an input method to the model. The model performs examinations impersonations detection with great accuracy. This success was attributed to appealing attributes like the extensive QR code capacity, compact print size, rapid scanning capability, durability against damage and the dynamic challenging profile questions algorithm which provides an extra layer of security by adding personalized questions that only the legitimate student would know the answers, reducing the risk of unauthorized access (ie. Enhanced Security), Unlike static security questions, dynamic profile questions are not stored in a database rather they are generated on demand, making it more difficult for attackers to predict and bypass the

authentication process (flexibility), Dynamic challenging profile questions cannot offer a more user-friendly authentication experience by allowing users to select questions that are relevant and memorable to them, this increase frustration to impersonators and increase compliance with security measures.

Since dynamic profile questions are unique to each student and can cover a wide range of personal attributes, they are less susceptible to social engineering attacks where attackers attempt to guess or obtain the answers through other means (ie. Reduced Vulnerability to Social Engineering) and dynamic challenging questions can help organizations meet regulatory requirements for strong authentication methods, such as those outlined in the Payment Card Industry Data Security Standard (PCI DSS) or the General Data Protection Regulation (GDPR) (ie. compliance with regulations). Overall, employing dynamic challenging questions for user authentication and impersonations detection can significantly enhance security while also improving the user experience and compliance with regulatory standards.

To assess the vulnerability of the system to guessing attacks, participating students were given the opportunity to disclose their profile information to impersonators at their convenience prior to coming at the examination venues for identification. This gave impersonators sufficient time to memorize the profile information of the targeted students, enabling them to potentially answer dynamic challenge questions generated by the system mechanism. The findings indicated that utilizing dynamic challenging questions derived from student profiles, particularly when accompanied by a proctor, effectively detects impersonations. Sharing of personal profile

information allowed impersonators to respond to 1 (25 %) or 2 (50%) questions correctly out of 4 questions. This suggested that 4 questions are effective for impersonations detection since they avoid guessing attack or correct responses by chance.

There were observed a significant possibility of $p < 0.25$ in the correct responses between an actual student and an impersonator. This implies that dynamic challenging questions generated from students' details, parents' or guardian' information, places of birth, course information and facilitators details makes it harder for impersonators to memorize all the details shared with an actual student hence it could be implemented for effective students identification and apparently be used for detection of impersonations in examinations. The suggested enhancement to the impersonations detection mechanism includes additional features which links to the database to retrieve information regarding students' profiles. Hence, if a student fails to enroll in a specific examination but shows up at the examination venue for authentication and eligibility verification, the proposed mechanism will recognize he(r) as ineligible to take the examination and classify he(r) as impersonator. Moreover, the suggested method for identifying impersonations generates a log file that monitors eligible students as they login. This enables the recording of examination attendance. Furthermore, a communication module has been incorporated to transmit security alerts to the security officer, enabling them to address security concerns at the specific venue where an impersonation incident is reported.

To demonstrate the implementation of the improved mechanism for detecting impersonations in traditional-in-class examinations, a mobile application was developed and installed in a mobile device which scanned the generated QR code image and display dynamic challenging questions generated by application on the mobile device screen. It took at most 2 seconds for the system to determine the eligibility of a single student for examinations. This suggests that 200 students can be verified within 33 minutes for one operator or 11 minutes if application operators are increased to 3. In addition the proposed mechanism or system have 0.02 (2%) FAR and 0 (0%) FRR while security of the mechanism is 0.98 (98%) and it is 100% convenient. Ultimately, the developed mobile application can conveniently verify examination eligibility while students wait in line to enter the examination venue, thereby capitalizing on widespread device availability that facilitates mobility.

5.2 Recommendations and Future Works

Future efforts can focus on exploring modalities for interacting with the developed dynamic challenging questions generation system such as integrating the model (system) with examinations' venues doors to automate the process of entering exams eligible students into examinations' venues. This will ultimately result in the construction of a comprehensive impersonations detection system that integrates with existing institutional systems, such as physical infrastructures (doors), student records systems, examination records systems, National Health Insurance System and payment system. This integration has the potential to be applied in building a big data structure that eventually can be utilized by a NLP model to create dynamic

questions based on complex student profile information and increase system reliability and security.

REFERENCES

- Abdullahi, M. B., Nura, Z. M, Jiya, L. M. (2019). Examination Eligibility Verification and Attendance System Using Quick Response Code. *i-manager's Journal on Digital Signal Processing, Vol. (6) INo. 3*, https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=EXAMINATION+ELIGIBILITY+VERIFICATION+AND+ATTENDANCE++SYSTEM+USING+QUICK+RESPONSE+CODE&btnG=
- Abu-Shanab E.A (2011). Education Level as a Technology Adoption Moderator. MIS Department, IT College Yarmouk University. DOI:10.1109/ICCRD.2011.5764029 accessed on April, 2024 at [13:00 PM]
- Ahmed H.S.A (2022). Facial Recognition Technology and Privacy Concerns. Accessed at <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2022/volume-51/facial-recognition-technology-and-privacy-concerns> on April, 2024 at [13:40 PM]
- AlHusain R, Alkhalifah A (2022). Evaluating knowledge-based security questions for fallback authentication. *PeerJ Comput Sci.* doi: 10.7717/peerj-cs.903. PMID: 35494806; PMCID: PMC9044221.
- Aramide, K. A., Ladipo, S. O. & Adebayo, I. (2015). *Demographic Variables and ICT Access as Predictors of Information Communication Technologies' Usage among Science Teachers in Federal Unity Schools in Nigeria* accessed at <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=3208&context=libphilprac> on 23rd March, 2024 [8:22 AM]

Akaranga, S.I. and Ongong, J.J. (2013). The Phenomenon of Examination Malpractice: An Examinationple of Nairobi and Kenyatta Universities. *Journal of Education and Practice* www.iiste.org ISSN 2222-1735 Vol.4, No.18, 87-97.

https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=The+Phenomenon+of+Examination+Malpractice%3A+An+Examinationple+of+Nairobi+and+Kenyatta+Universities&btnG=

Akinola1, O.A , Abayomi-Alli, A. & Adeniyi, R. A (2015). Development of a Microcontroller Based Fingerprint Examination Access Control System. *African Journal of Computing & ICT*, Vol 8. No. 2 Issue 2, 145-152. ISSN 2006-1781 www.ajocict.net.

https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Developm+ent+of+a+Microcontroller+Based+Fingerprint+Examination+Access+Co+ntrol+System&btnG=

Anderson, W. (nd). Cheating Control On Examinations. *Journal of Agronomic Education*, Vol. 10,1981. Accessed at

<https://www.agronomy.org/files/publications/jnrlse/pdfs/jnr010/010-01-0013.pdf>on 13th August, 2022 at [12:45] <https://www.fraud-magazine.com/article.aspx?id=4295019499>

Anandhavalli D, Devi N, Deepshika H, Priyadharshini M (2020). Automated Fraud Detection Framework in Examination Halls. *International Research Journal of Engineering and Technology (IRJET)*. www.irjet.net. Volume: 07 Issue: 03

- Anthony J. B. (2012). Forensic Science: Fundamentals and Investigation, 2012 Update, Capstone Edition. [Online] Centage Learning Publishers. Available from <http://www.cengage.com/forensicscience> [Accessed on December, 2023].
- Al Kilani, M. and Kobziev, V. (2016) An Overview of Research Methodology in Information System (IS). *Open Access Library Journal*, 3: e3126. <http://dx.doi.org/10.4236/oalib.1103126>
- Baijnath N., Singh D. (2019). *Examination cheating: Risks to the quality and integrity of higher education. S Afr J Sci.* 2019;115(11/12), Art. #6281, 6 pages. <https://doi.org/10.17159/sajs.2019/6281> accessed on 11th August, 2022 at [10:09]
- Bait. A, Garko and Ahmad. A (2017). Design And Modeling Of A Student Verification System In An Examination In Nigeria Using Biometric Fingerprint Technology. *International Journal of Advanced Academic Research / Sciences, Technology & Engineering* Vol. 3, Issue 7, 1-16. ISSN: 2488-9849. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Design+And+Modeling+Of+A+Student+Verification+System+In+An+Examination+In+Nigeria+Using+Biometric+Fingerprint+Technology&btnG=
- Bangor, A., Kortum, P., Miller, J.: Determining what individual SUS scores mean: Adding an adjective rating scale. *J. Usability Stud.* 4(3), 114–23 (2009)
- Binu, D, Bhuvana, D, Karthika, B. and Kayalvizhi, M. (2018). Bi-Modal Examination Hall Authentication System. *Journal of Xi'an Shiyou*

University, Natural Science Edition. VOLUME 18 ISSUES 02, 114-117.

[https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Bi-](https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Bi-Modal+Examination+Hall+Authentication+System&btnG=)

[Modal+Examination+Hall+Authentication+System&btnG=](https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Bi-Modal+Examination+Hall+Authentication+System&btnG=)

Brouwer-Janse et al (1997). User interface for young. The widespread use and merging of advanced information, communication and entertainment systems entices. The human computer interaction (HCI) community to broaden its focus to the population at large and in particular to two outstanding groups: Children and the elderly. *Philips Research Laboratories, Institute for Perception Research Eindhoven*. Accessed at <https://dl.acm.org/doi/pdf/10.1145/245129.245133>

Corry, M.D., Frick, T.W., Hansen, L.: User-centered design and usability testing of a web site: An illustrative case study. *Educ. Technol. Res. Dev.* 45(4), 65–76 (1997)

Chala, W (2021). Perceived seriousness of academic cheating behaviors among undergraduate students: an Ethiopian experience. *Chala International Journal for Educational Integrity* (2021) 17:2

<https://doi.org/10.1007/s40979-020-00069-z>. Accessed on 12th August, 2022 at [17:45]

Diedenhofen, B. and Musch, J. (2016). Page Focus: Using paradata to detect and prevent cheating on online achievement tests. *Behav Res* (2017) 49:1444–1459, DOI 10.3758/s13428-016-0800-7

Diana Starovoytova Madara* Saul Sitati Namango Harrison Katana (2017). *Cheating Theories*

De Aquino, T and Yambi UGS, C (2020). *Assessment and Evaluation In Education*.

Accessed at

https://www.researchgate.net/publication/342918149_ASSESSMENT_AND_EVALUATION_IN_EDUCATION/link/5f0d737aa6fdcc547aee9fb3/download on 13th August, 2022 at [12:45]

Emily, S. (2019). “Understanding from Machine Learning Models”. *British Journal for the Philosophy of Science* 73 (1):109-133. Google Scholar. Accessed on May, 2024 at [13:02 pm]

Eziechina, A. M, Ugboaja, U.C, Esiagu, U.E (2017). Closed-Circuit Television Surveillance: An Antidote To Examination Malpractice in High Institutions In Nigeria. *American Journal of Engineering Research (AJER)* Volume-6, Issue-12, pp-247-251. e-ISSN: 2320-0847 p-ISSN : 2320-0936

https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=%29.+Closedcircuit+Television+Surveillance%3A+An+Antidote+To+Examination+Malpractice+in+High+Institutions+In+Nigeria&btnG=

Elaskariab, S, Imrana , M. Elaskric , A. and Almasoudi, A (2021). Using Barcode to Track Student Attendance and Assets in Higher Education Institutions. *Procedia Computer Science* 184 (2021) 226–233. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Using+Barcode+to+Track+Student+Attendance+and+Assets+in+Higher+Education+Institutions&btnG=

Farisi M. I. and Surabaya, T. (2013). Academic Dishonesty In Distance Higher Education: Challenges And Models For Moral Education In The Digital

Era. *Turkish Online Journal of Distance Education-TOJDE* Volume: 14
Number: 4 Article 1, 176-195.

https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Academic+Dishonesty+In+Distance+Higher+Education&btnG=

Forgas, R. Lancaster, T, Sastre, A and Negre, J. (2021). Examination cheating and academic integrity breaches during the COVID-19 pandemic: An analysis of internet search activity in Spain. *Journal of the Academy of Nutrition and Dietetics* Volume 7, Issue 10. Accessed at

<https://www.sciencedirect.com/science/article/pii/S2405844021023367> on 10th
August, 2022 at [12:45]

Garko A.B., and Ahmad, A. (2017). Design and Modeling of A Student Verification System in an Examination in Nigeria Using Biometric Fingerprint Technology. *International Journal of Advanced Academic Research / Sciences, Technology & Engineering* / ISSN: 2488-9849 Vol. 3, Issue 7. ISSN: 2488-984

Handbook of Research on Transnational Higher Education (2 Volumes).

<https://www.igi-global.com/book/handbook-research-transnational-higher-education/75837#table-of-contents> 19th Nov. at [2022 12:05 pm]

Hoque, MD. J , Ahmed, Md. R, Uddin, Md. J and Faisal, M.M.A (2020). Automation of Traditional Examination Invigilation using CCTV and Bio-Metric. (*IJACSA*) *International Journal of Advanced Computer Science and Applications*, Vol. 11, No. 6, 391-399.
https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=%29.++A

utomation+of+Traditional+Examination+Invigilation+using+CCTV+and
+Bio-Metric&btnG=

Iwasokun G. B , Omomule, T. G , and Akinyede, O.R (2018). Design of a Framework for Computer-Based Examination Invigilation Using Fingerprint and Iris Technologies. *2 nd International Conference on Information and Communication Technology and Its Applications (ICTA 2018)*, 177-183.

https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Design+of+a+Framework+for+Computer-Based+Examination+Invigilation+Using+Fingerprint+and+Iris+Technologies&btnG=

Isinkaye, F. O, Soyemi, J and Arowosegbe, O.I (2020). An Android-based Face Recognition System for Class Attendance and Malpractice Control. *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 18, No. 1, 79-83.

https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=An+Android-based+Face+Recognition+System+for+Class+Attendance+and+Malpractice+Control&btnG=

John, B. (2020). SUS - A quick and dirty usability scale. Research gate. Accessed at on at: <https://www.researchgate.net/publication/228593520> on september 2023.

Kothari, C. and Garg, G. (2014). Research methodology Methods and Techniques. 3rd ed. New Delhi: New Age International (P) Ltd., p.63.

- Kobiowu, S. V. and Alao, F (2015). The Challenges of Examination Management in the Developing Societies: The Nigerian Scenario. *International Journal of African & African American Studies Vol. IV, No. 2, Jul 2005, 39-47.*
https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=The+Challenges+of+Examination+Management+in+the+Developing+Societies%3A+The+Nigerian+Scenario&btnG=
- Lazarus, L., Mokula, D and Lovemore, N (2014). Forms, Factors and Consequences of Cheating In University Examinations: Insight from Open and Distance Learning Students. *Turkish Online Journal of Distance Education-TOJDE October 2014 ISSN 1302-6488 Volume: 15 Number: 4 Article 17.*
- Lourde M.R., Dushyant K. (2010). Fingerprint Identification in Biometric Security System. *Journal of Computer and Electrical Engineering*, 2(5), 852-855.
- Lee,J., Jinyoung, R., Park, K. and Henning, M. (2020). *Using technologies to prevent cheating in remote assessments during the COVID-19 pandemic.*
 DOI: 10.1002/jdd.12350
- Lee, Myungjoon (1994). "Plato's philosophy of education: Its implication for current education"*Dissertations (1962 - 2010).* Accessed via Proquest Digital Dissertations. AAI9517932 at
- Lewis, S (2017). *Prototyping Model.*
<https://www.techtarget.com/searchcio/definition/Prototyping>
 Model#:~:text=The%20prototyping%20model%20is%20a,or%20product%20can%20be%20de eloped on 10th August, 2022 at [12:45]

- Madara, D and Namango, S (2016). Faculty Perceptions on Cheating in Examinations in Undergraduate Engineering. *Journal of Education and Practice* ISSN 2222-1735 (Paper) ISSN 2222-288X (Online). Vol.7, No.30, 2016. Available at <http://www.iiste.org/> on 10th August, 2022 at [12:45]
- Midlands, E.T, Matamande, W. and Mandimika, E. (2014). Exploring management strategies to reduce cheating in written examinations: case study of Midlands State University. *Journal of Case Studies in Education*, 1-13
- MO Oladele, TM Adepoju, EO Omidiora, AA Sobowale, OA Olatoke (2020). An offline yorùbá handwritten character recognition using support vector machine, *Malaysian Journal of Computing (MJoC)*, 5 (2). pp. 504-514. ISSN 2600-8238. Accessed at <https://mjoc.uitm.edu.my>
- MNMA (2024). *Genera Examination Regulations and Guidelines 2nd edition, 2024*. The Mwalimu Nyerere Memorial Academy, Dar es Salaam, Tanzania.
- MM Rufai, JO Adigun, NA Yekini (2012). A biometric model for examination screening and attendance monitoring in Yaba College of Technology. *World of Computer Science and Information Technology Journal* 2 (4), 120-124
- Nagal, R, Nemkul, P, Mandal, D, Kumar, N and Joseph, A (2017). Android based Secure Examination Management System to Prevent Impersonations. *International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS) 1 st Special Issue on Engineering and Technology* . Volume VI, Issue VS, 2278-2540. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Android+

based+Secure+Examination+Management+System+to+Prevent+Impersonations&btnG=

Njoku, N.C, Njoku, D.I. (2016). Curbing Examination Malpractice in Secondary Schools in Nigeria through Moral Education. *Research on Humanities and Social Sciences* Vol.6, No.18, 161-169. www.iiste.org ISSN (Paper) 2224-5766 ISSN (Online) 2225-0484 (Online). https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Curbing+Examination+Malpractice+in+Secondary+Schools+in+Nigeria+through+Moral+Education&btnG=

Noorbehbahani F, Mohammadi, A and Aminazadeh, M (2022). *A systematic review of research on cheating in online examinations from 2010 to 2021*. Accessed at <https://link.springer.com/article/10.1007/s10639-022-10927-7> on 13th August, 2022 at [12:45]

Onaolamipo, A.T (2014). Development of A Computerized Biometric Control Examination Screening And Attendance Monitoring System With Fees Management. *World of Computer Science and Information Technology Journal (WCSIT)* ISSN: 2221-0741 Vol. 4, No. 6, 76-81. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Development+of+A+Computerized+Biometric+Control+Examination+Screening+And+Attendance+Monitoring+System+With+Fees+Management&btnG=
NSTC Subcommittee on Biometrics (2006). *Fingerprint Recognition*. National Science and Technology Council.

Odejobi O.A. and Clarke, N.L. (2009). Implementing Biometrics to Curb Examination Malpractices in Nigeria. *Advances in Communications*,

Computing, Networks and Security: Proceedings of the MSc/MRes programmes from the School of Computing, Communications and Electronics.

https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Implementing+Biometrics+to+Curb+Examination+Malpractices+in+Nigeria.+Advances+in+Communications%2C+Computing%2C+Networks+and+Security&btnG=

Onyema, E.M, Eucheria, A.U, David, N.A, Isa, A, Alsayed, A.O and Naveed, Q.N (2019). The Role of Technology in Mitigation of Examination Malpractices in West Africa. *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 7, Issue 10, 3990-4002. DOI: 10.15680/IJRCCE.2019. 0710007 (https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=The+Role+of+Technology+in+Mitigation+of+Examination+Malpractices+in+West+Africa&btnG=)

Onuka A, and Durowoju E, (2011). Curtailing Examination Fraud for Improved Quality Assurance in the African Examinationining System. *Journal of Educational Assessment in Africa*, Vol (6), (27-38). <https://www.google.com/search?client=firefox-b-Examination+Fraud+for+Improved+Quality+Assurance+in+the+African+Examinationining+System>.

ParulSindha (2012). Minutiae Based Fingerprint Recognition System. *Indian Journal of Research*, 1(12), 88-90.

Patton, M. (2015) *Qualitative Research and Evaluation Methods. 4th Edition, Sage Publications, Thousand Oaks.*

Permana I. S. , Hidayat T. and Mahardiko R. (2021). Mobile Phone Scanner Technology Adoption – A Comparison Analysis. *Conference: International Conference on Applied Science and Technology At: Padang, Indonesia DOI:10.2991/aer.k.211129.071* accessed https://www.researchgate.net/publication/344364324_Mobile_Phone_Scanner_Technology_Adoption_-_A_Comparison_Analysis at April, 2024 [17:48 pm]

P. Modal (2022). *Plato's Theory of Education. Accessed at* <https://www.yourarticlelibrary.com/education/platos-theory-of-education/40135> on 13th August, 2022 at [12:45].

Rufai M.M, Adigun J. O, Yekini N. A (2012). A Biometric Model For Examination Screening and Attendance Monitoring In Yaba College Of Technology. *World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 4, 120-124.*
https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=A+Biometric+Model+For+Examination+Screening+And+++++Attendance+Monitoring+In+Yaba+College+Of+Technology&btnG=

Rădulescu, G. and Popescu, C. (2014). About Barcode Technology Case study: Computerization of a Library. *BULETINUL Universității Petrol – Gaze din Ploiești*, No. 3/2014, 7-14.

https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=About+Barcode+Technology+Case+study%3A+Computerization+of+a+Library&btnG=

Richard, G. (2022). "A Framework Comparison: .NET and Laravel". Honors Theses, University of Nebraska-Lincoln. 497. Available at <https://digitalcommons.unl.edu/honorstheses/497> accessed on May, 2024 at [5:30 AM]

Salehi, M and Gholampour, S (2021). Cheating on examinations: Investigating Reasons, Attitudes, and the Role of Demographic Variables. *Journals.sagepub.com/home/sgo* DOI: 10.1177/21582440211004156

Saheed, Y.K, Hambali, M.A, Adeniji, I. A and Kadr, A.F (2017). Fingerprint Based Approach for Examination Clearance in Higher Institutions. *FUOYE Journal of Engineering and Technology, Volume 2, Issue 1*, 47-50. ISSN: 2579-0625 (Online), 2579-0617 (Paper). https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Fingerprint+Based+Approach+for+Examination+Clearance+in+Higher+Institutions&btnG=

Saheed, Y.K, Hambali, M.A, Adediji, A. A. and Adeniji, I.A. (2016). Attendance Management System Using Barcode Identification on Students' Identity Cards. *The Pacific Journal of Science and Technology*, Volume 17. Number 2. November 2016 (Fall), 224-230. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Attendance

e+Management+System+Using+Barcode+Identification+on+Students%
E2%80%99+Identity+Cards&btnG=

- Setiawana, N., Suharjitoa and Diana (2019). A Comparison of Prediction Methods for Credit Default on Peer to Peer Lending using Machine Learning: 4th International Conference on Computer Science and Computational Intelligence 2019 (ICCSCI), 12–13 September 2019. *Procedia Computer Science* 157 (2019) 38–45. Available at <https://www.sciencedirect.com/science/article/pii/S1877050919310683> accessed on May, 2024 at [5:30 AM]
- Shen, J, Cheng, K Bieber, M and Hiltz, S. R (2004). Traditional In-class Examination vs. Collaborative Online Examination in Asynchronous Learning Networks: Field Evaluation Results. *Collaborative Hypermedia Research Lab Information Systems Department New Jersey Institute of Technology*.
- Starovoytova, D. and Namango, S (2016). Factors Affecting Cheating-Behavior at Undergraduate-Engineering. *Journal of Education and Practice* www.iiste.org ISSN 2222-1735 (Paper) ISSN 2222-288X (Online) Vol.7, No.31, 2016. Available at <https://www.iiste.org> on 11th August, 2022 at [13:52]
- Sri Shimal Das, JhunuDebbarma (2011). Measure for Enhancing Automated Teller Machine Security in Indian E-banking System. *International Journal of Information and Communication Technology Research*, 1(5), 197- 201.
- State of University Education in Tanzani (2018). Accessed at <https://www.tcu.go.tz> on 10th August, 2022 at [12:45]

Tanzania Commission for Universities (2021/2022). *Undergraduate Admission Guidebook*. TCU

Tashildar, A., Shah, N., Gala, R., Giri, T., and Chavhan, P. (2020). APPLICATION DEVELOPMENT USING FLUTTER. *International Research Journal of Modernization in Engineering Technology and Science* Volume: 02/Issue: 08/August-2020. Available at https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=eatures+of+Flutter+frmaework&btnG= accessed on May, 2024 at [5:30 AM]

Tiong, L and Lee, H (2021). E-cheating Prevention Measures: Detection of Cheating at Online Examinations Using Deep Learning Approach - A Case Study. *Journal Of Latex Class Files*, Vol. Xx, No. Xx, Jan 2021

<https://epublications.marquette.edu/dissertations/AAI9517932>on 13th August, 2022 at [12:45]

Tomas de Aquino Yambi, C. (2022). "Teacher Training vs. Trainer Training in Education," *International Journal of Research and Innovation in Social Science*, *International Journal of Research and Innovation in Social Science (IJRISS)*, vol. 6(8), pages 709-715, accessed on December, 2023 [13:30].

TCU (2021). VitalStats. Available at <https://www.tcu.ac.tz>

T. Ramu, T. Arivoli (2013). A Framework Of Secure Biometric Based Online Examination Authentication: An Alternative to Traditional Examination. *International Journal of Scientific & Engineering Research*, Volume 4, Issue 11, November-2013 52 ISSN 2229-5518

The Mwalimu Nyerere Memorial Academy, Prospectus (2021/2022). Available at

<https://www.mnma.ac.tz>

The Mwalimu Nyerere Memorial Academy (2023/2024). *Prospectus*. Available at

<https://www.mnma.ac.tz>

The Open University of Tanzania (OUT), Prospectus (2021/2022). Available at

<https://www.out.ac.tz>

The Tanzania Commission for Universities (2022). *VitalStats on University*

education in Tanzania, 2022),

<https://www.tcu.go.tz/sites/default/files/VitalStats%202021.pdf> on 19th

Nov. at [2022 12:05 pm].

The Tanzania Commission for Universities (2021). Undergraduate Admission

Guidebook for 2021/2022 Academic year: For Holders of Ordinary

Diploma or Equivalent Qualifications. ISBN 978-9976-9353-1-4. Dar es

Salaam, Tanzania.

Uchenna, M.M, Funke, I. A (2015). Empirical Investigation into the Causes, Forms

and Consequences of Examination Malpractice in Nigerian Institutions of

Higher Learning. *International Journal of Novel Research in Humanity*

and Social Sciences Vol. 2, Issue 1, pp: (52-62), Month: January -

February 2015, Available at: www.noveltyjournals.com accessed

Ullah A., Xiao H., Barke T. (2019). A Dynamic Profile Questions Approach to

Mitigate Impersonations in Online Examinations. *J Grid Computing*

(2019) 17:209–223. Accessed

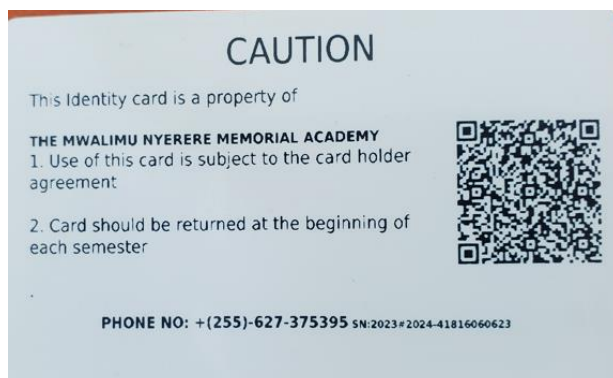
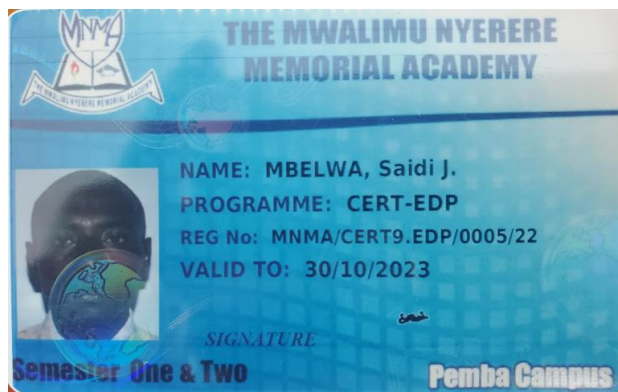
at <https://doi.org/10.1007/s10723-018-9442-6>

- Vivian, N. I, Ise, O.A Orobor (2020).Face Recognition Service Model for Student Identity Verification Using Deep Neural Network and Support Vector Machine (SVM). *Int J Sci Res CSE & IT*, 6 (4) : 11-20. ISSN: 2579-0625 (Online), 2579-0617 (Paper).
https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Face+Recognition+Service+Model+for+Student+Identity+Verification+Using+Deep+Neural+Network+and+Support+Vector+Machine+%28SVM&btnG=
- Wedawatta, G., Ingirige, B. and Amaratunga, D. (2011). Case Study as a Research Strategy: *Investigating Extreme Weather Resilience of Construction SMEs in the UK. 7th Annual International Conference of International Institute for Infrastructure, Kandalama, July 2011, 1-9.*
- Yamane, T. (1967). *Statistics: An Introductory Analysis. 2nd Edition*, Harper and Row, New York.
- Zubairu H* , Mohammed I , Etuk S , Babakano F and Ilyasu A (nd). *A Context-Aware Framework for Continuous Authentication in Online Examination. ICT4NDS2021: ICT and Sustainability in the 5th Industrial Revolution*. Proceedings of the 2nd International Conference on ICT for National Development and Its Sustainability, Faculty of Communication and Information Sciences, University of Ilorin, Ilorin, Nigeria- 2021.

APPENDICES

Appendix1: Evidence of using manual Identification documents in selected public higher learning institutions in Tanzania

1 (a) The Mwalimu Nyerere Memorial Academy (MNMA) Student Identity Card



1(b) . The Local Governemnt Training Institute (LGTI) Examination Coupon



Appendix 2: Evidence of using other identification documents apart from institutional identity documents during examinations



THE UNITED REPUBLIC OF TANZANIA

THE MWALIMU NYERERE MEMORIAL
ACADEMY



When replying please mention:

Ref. No: MNMA/SG/VOL. III/159

26th May, 2024

INTERNAL MEMO

ALL STUDENTS
THE MWALIMU NYERERE MEMORIAL ACADEMY

RE: TEST TWO OF SEMESTER II (SEPTEMBER INTAKE) AND SEMESTER I (MARCH INTAKE) COMMENCING ON 27th MAY, 2024

Kindly refer to the above heading.

2. According to the Almanac for academic year 2023/2024, TEST TWO for the Second Semester (September intake) and First Semester (March Intake) will be conducted from Monday, 27th May, 2024 to, Friday 31st May 2024. **ALL STUDENTS** are reminded to observe the following.

- (1) Students eligible to sit for TEST TWO are only those with complete registration.
- (2) Every student should have a **VALID IDENTITY CARD (ID)** of the Mwalimu Nyerere Memorial Academy.
- (3) **First Year (September Intake)** Students whose records are in ARMS should use their IDs from SEMESTER ONE. Those who have paid their tuition fees but their IDs are not yet issued should bring along **authentic EVIDENCE OF HAVING PAID THE FEES** attached with a passport size photograph for easy identification.
- (4) **First Year (March Intake 2024)** Students whose records are in ARMS and do not have IDs should use their registration forms attached with a passport size photograph for easy identification.
- (5) **Second and Third Year** students who have paid their tuition fees but their IDs are not yet printed should bring along an **authentic EVIDENCE OF HAVING PAID THE FEES** accompanied with the ID from Semester One.
- (6) Any **OTHER TYPES OF IDENTIFICATIONS ARE STRICTLY NOT ALLOWED** for admission in the examination rooms.
- (7) During the Test, everyone should adhere to the Examination Regulations. As a reminder, Examination regulations have been posted at the entrance of every examination room for your attention.

3. On behalf of the Management I wish you good luck as you prepare for the Test.

4. Yours sincerely,

Prof. Richard Y.M. Kangaliwa

DEPUTY RECTOR – ACADEMIC, RESEARCH AND CONSULTANCY

cc: Rector
Deputy Rector – Planning, Finance and Administration

Appendix 3: Data Collection Tools



The Open University of Tanzania
Affordable Quality Education for All

**FACULTY OF SCIENCE, TECHNOLOGY AND ENVIRONMENTAL
 STUDIES (FSTES)**

**DEPARTMENT OF MATHEMATICS, INFORMATION AND
 COMMUNICATION TECHNOLOGY**

COURSE CODE: OCS 610

Student's Information

Student Full Name	Registration Number	Phone Number	Email Address
Domition, JassonLwangisa.	PG202086723	0777 654770	jassondomition@gmail.com

Supervisor's Information

Supervisor's Full Name	Phone Number	Email Address
Dr. Rogers Bhalalusesa	0679950442	Rogers.bhalalusesa@out.ac.tz

3 (a) An Interview Guide

1. SPECIFIC OBJECTIVE ONE: Identifying technologies suitable for detecting impersonation during traditional-in-class examinations.

2. INTRODUCTION: This Interview Guide Will Help to Explore the Various Aspects of Impersonation Detection Technologies and Their Features in depth in the context of Traditional-In-Class Examinations along with their implementation details.

3. PARTICIPANTS: ICT STAFF (Academics and Non-Academics)

4. PRINCIPAL RESEARCH QUESTION: What are the technologies that can be used to detect impersonation during traditional-in-class examinations?

5. SUB-ENABLING RESEARCH QUESTIONS:

A. Overview:

- i. What is your experience and expertise in the area of impersonation detection technologies?
- ii. Main challenges associated with detecting impersonation during traditional in-class examinations, and why is it important to address this issue?

B1. Knowing the background: Kindly describe currents commonly impersonation detection techniques in traditional-in-class examinations. Outline the limitations associated with these techniques.

B2. Number of students in exam venue. ie maximum Venue capacity, number of invigilators per venue and maximum authentication time per students, recommendations on current authentication time and efficiency of existing auth. Techniques. Further improvements required?

B3: what information you expected a student to know so that he/she can be the correct one?

B4: Can lectures poses such knowledge given current number of students and environment? Give reasons and recommendations.

C. Inspiration for Impersonation Detection: What are the significance of detecting traditional-in-class impersonations? And what will happen if this fraud is not addressed?

D. understanding traditional-in-class Impersonation Detection Technologies: What is meant by impersonation detection technologies and what is their purpose in in traditional crass room contexts?

E. Identifying Common Technologies:

- i. What emerging technologies or tools do you believe hold promise for improving the detection of impersonation during traditional-in-class examinations?
- ii. What are the most common prominent technologies used for traditional-in-class examinations impersonation detection?
- iii. May you in summary describe each of these technologies and their important features?
 - ❖ Working mechanism and or components
 - ❖ Reliability and response time
 - ❖ Cost
 - ❖ Degree of User acceptance and reasons
 - ❖ Availability
 - ❖ Initial setup cost (requirements)

- ❖ Recommendations as per institution's capability and utilization of existing infrastructures such as mobile phones, students IDs etc.

E1. QR CODE Technology:

- i. May you explain how QR Code technology work in this context?
- ii. What are the key features of a QR Code technology for detecting traditional-in-class examinations impersonations?
- iii. Can you List the potential pros and cons of applying QR Code technology for detecting traditional-in-class examinations impersonations in your institution?
- iv. How do QR Code technology (facilitate the detecting traditional-in-class examinations impersonations?

E2: Knowledge Analysis:

- i. How does Knowledge Analysis facilitate the detection of traditional-in-class examinations impersonations, and what types of knowledges are typically analyzed?
- ii. Can you explain the distinguished Knowledge Analysis technologies?
- iii. In what ways can Knowledge Analysis technologies contribute to impersonation detection during traditional-in-class examinations?
- iv. What are the specific Knowledge patterns that these technologies analyze?
- v. Algorithm for knowledge analysis and components
- vi. Model for knowledge analysis
- vii. Guaranteed security and privacy
- viii. Static QNS vs dynamic questions: sample systems for static QNS & dynamic QNS and recommendations as per pros and cons of each

- ix. Requirements (S/W &H/W plus skills and frameworks) for their development
- x. How to enforce students adapt and the system before final/SE?
- xi. Important information to capture student identity (Authentication)

E3: Machine Learning and AI

How does a machine learning and artificial intelligence contribute to improving impersonation detection in traditional-in-class examinations?

Can you provide examples of machine learning algorithms or AI models used in this context?

How does machine learning and artificial intelligence enhance impersonation detection in traditional-in-class examinations?

E4. Biometric Technologies:

- i. May you explain how biometric technologies like iris recognition or fingerprint detection work in this context?
- ii. What are the key features of a biometrics for this detecting traditional-in-class examinations impersonations?
- iii. Can you List the potential pros and cons of applying biometrics for detecting traditional-in-class examinations impersonations in your institution?
- iv. How do biometric technologies (e.g., iris recognition or fingerprint detection) facilitate the detecting traditional-in-class examinations impersonations?

F: Key Features of Impersonation Detection Technologies:

F1. Accuracy and False Positives:

- i. How do these technologies ensure accurate detection while minimizing false positives?

- ii. What metrics are commonly used to measure accuracy in impersonation detection in traditional-in-class examinations?

F2. Real-time Detection:

- i. Is real-time detection an essential feature of impersonation detection technologies? If so, how is it achieved?
- ii. Are there any latency concerns with real-time detection?

F3. Scalability

- i. How do these technologies scale to accommodate various settings, such as small classrooms or large lecture halls?
- ii. Are there scalability challenges associated with certain technologies?

F4. User-Friendly Interfaces:

- i. To what extent are these technologies user-friendly for both educators and students?
- ii. Are there any user interface features that enhance usability?

F5: Privacy and Data Protection

- i. What measures are in place to protect the privacy of individuals when using impersonation detection technologies?
- ii. How is sensitive data handled and stored?

G: Integration and Implementation

G1 Compatibility with Existing Systems

- i. Can these technologies seamlessly integrate with existing educational systems and infrastructure?
- ii. Are there any compatibility challenges?

- iii. Are there specific technologies or tools that are commonly integrated into physical classroom exams for impersonation detection purposes?
- iv. How are impersonation detection technologies integrated with the overall examination process in traditional-in-class settings?
- v. Are there any specific workflows or protocols?
- vi. What challenges or limitations are associated with the implementation of impersonation detection technologies in traditional-in-class exams?
- vii. Are there any common issues that institutions face?
- viii. State of network/internet infrastructure at the institution and national at large
- ix. State of H/W infrastructure at the institution eg. Application Server availability, virtualization, type of cloud computing services available and government/institutional ICT policy (its state) on institutions cloud computing services, technical expertise (inhouse/outsource)
- x. Academics knowledge and perceptions on Mobile apps operations
- xi. Management knowledge and perceptions on Mobile apps operations
- xii. Availability of budget to support this efforts eg. Buying smartphones where the app is installed, Pay for Internet Bills/LAN configurations etc.

G2. Cost and Resource Considerations:

- i. What are the typical costs associated with implementing impersonation detection technologies?
- ii. How do institutions allocate resources effectively for implementation?
- iii. What are some key factors to consider when selecting a technology solution for detecting impersonation, such as cost-effectiveness, scalability, and accuracy?

- iv. Will (management) to support this efforts

G3. Training and Support

- i. What kind of training and support are required for educators and administrators when implementing these technologies?
- ii. Are there ongoing maintenance and support needs?
- iii. How can educators and students be educated and trained to understand and cooperate with the use of impersonation detection technologies in a classroom setting?

G4. Security:

What steps should be taken to ensure the security and integrity of data collected during the impersonation detection process?

H. Future Trends and Challenges

- i. What are some emerging trends or innovations in impersonation detection technologies?
- ii. How are these technologies evolving to meet new challenges?
- iii. Can you discuss any real-world case studies or success stories where technology was effectively used to prevent impersonation in traditional in-class examinations?

INTERVIEW GUIDE FOR SPECIFIC OBJECTIVE 2

SPECIFIC OBJECTIVE 2: Developing an improved mechanism for detecting impersonations in the context of traditional-in-class examinations (QR CODE AND DCQBSP)

2. INTRODUCTION: This interview guide should assist in exploring the requirements suitable for developing an improved mechanism that detects

impersonation in traditional in-class examinations and gathering valuable insights for this objective.

3. PARTICIPANTS: ICT Staff, Directors-ARC, Academic Staff and Ict Officers

4. PRINCIPAL RESEARCH QUESTION: How to develop an improved mechanism for detecting impersonations in the context of traditional-in-class examinations?

5. SUB-ENABLING RESEARCH QUESTIONS:

6. Introduction: introducing a research focus on developing an improved mechanism for detecting impersonations in traditional in-class examinations.

A. Existing impersonation detection mechanisms for the traditional-in-class examinations

- i. Are there any existing mechanisms that serve as a foundation for developing an improved mechanism for impersonation detection in the context of traditional-in-class examinations?
- ii. Can you describe any notable examples and their key components?
- iii. How these components works to produce results?
- iv. What students' information are crucial for determining his or her identity with great accuracy?
- v. In case an impersonation is detected what institutional syndicate is dedicated to handling impersonation and related irregularities?
- vi. Have you observed impersonators harming or trying to harm the invigilator? Why do you think was the reason?
- vii. What should be done in future to detect impersonation?
- viii. In your opinion, Should impersonation be prevented?

- ix. Do you believe that students have been engaging in impersonations during traditional-in-class examinations? Why so?
- x. Can you describe any real incident where you observed impersonation?

B. Components and Features of the impersonation detection mechanism:

- i. What are the essential components that constitute an impersonation detection mechanism in the context of traditional in-class examinations? (knowledge based)
- ii. Can you provide a brief description of each component's function and role?

C. Technological Integration:

- i. How does technology play a role in the design of the of impersonation detection mechanism? Are there specific technologies, such as QR code and dynamic challenging questions (Knowledge) that are integral in this mechanism?
- ii. What is the rationale behind the selection of each technology?

D. Security Measures:

- i. Is it possible appropriate to integrate more than one components such as QR code technology and dynamic challenging questions in same mechanism for detecting traditional-in-class examinations impersonations?
- ii. For this case, what are the key components that make up an improved mechanism for impersonation detection?
- iii. Could you briefly describe the two components integrations and state each component's role and function?
- iv. How do these technologies play a role in the mechanism? (e.g., QR Codes and dynamic challenging questions (knowledge))

- v. Are QR Codes and dynamic challenging questions (knowledge)) technologies effective in this context?

E. User-Friendliness

- i. How user-friendly is this mechanism usable for both educators and students?
- ii. Are there considerations for minimizing disruptions during the exam process?

F. Scalability and Adaptability:

How much will it be adaptable to various educational settings and institutions including yours If this mechanism is implemented as a software package?

G. required data to implement the dynamic challenging questions based on student's profile:

What technology and data area required to dynamically generate dynamic challenging questions based on student profile?

H. Real-time Detection:

- i. Does the mechanism in G above offer real-time impersonation detection during the traditional-in-class examinations, and if so, how is this achieved?
- ii. What are the advantages of real-time detection?

I. Implementation and Challenges:

- i. How does the mechanism integrate with existing examination processes and systems in the institution?
- ii. Are there any specific challenges or considerations during integration?

J. Accuracy and False Positives:

How is the accuracy of the impersonation detection ensured, while minimizing false positives?

INTERVIEW GUIDE FOR SPECIFIC OBJECTIVE 3

SPECIFIC OBJECTIVE 3: How to evaluate an improved mechanism for detecting impersonations in the context of traditional-in-class examinations?

2. INTRODUCTION: These interview questions should help to assess and evaluate the mechanism for detecting impersonations in traditional in-class examinations comprehensively, gathering insights into its effectiveness and potential areas for improvement.

3. Participants: ICT staff, ARC, students and academic staff

A. Understanding the mechanism

- i. What is the primary objective of this mechanism for detecting impersonations in traditional in-class examinations?
- ii. Can you provide examples or scenarios where the mechanism prototype would be applied?
- iii. How does the mechanism prototype address specific use cases or challenges in its intended domain?
- iv. Can you describe the key components and features of this mechanism that are essential for impersonation detection?
- v. How is this mechanism currently being implemented in traditional in-class examinations, and in what educational settings or institutions?
- vi. What motivated the development or evaluation of this mechanism, and why is it important to assess its effectiveness?
- vii. Does the mechanism have specific technologies such as QR CODES and dynamic challenging questions based on student profile or data analytics involved?

- viii. How do these technological elements contribute to the mechanism effectiveness in detecting impersonations?

B. User Experience and Interface:

- i. How user-friendly is the mechanism prototype?
- ii. Have user interface design and user experience considerations been taken into account?
- iii. What feedback or observations do you have regarding the ease of use for both administrators and end-users?

C. Performance and Efficiency:

- i. How has the performance of the mechanism prototype been tested or measured? What were the results?
- ii. Are there specific metrics or benchmarks that were used to evaluate the efficiency of the mechanism prototype?
- iii. What are the key performance metrics used to measure the success of the mechanism?
- iv. How does it compare to existing methods in terms of accuracy and efficiency?

D. Testing Protocols:

- i. How is the effectiveness of the impersonation detection mechanism tested and evaluated?
- ii. Are there specific testing protocols or benchmarks used?

E. Integration and Compatibility:

- i. How well does the mechanism prototype integrate with existing systems or processes within its intended environment?

- ii. Are there compatibility considerations with other tools or technologies that need to be addressed?

F. User Feedback and Adaptability:

- i. Have users provided feedback during the evaluation of the prototype, and if so, what were their main comments or suggestions?
- ii. How adaptable is the mechanism prototype to user needs and potential changes in the future?

G. Security and privacy

- i. What security measures and protocols are in place within the mechanism to prevent impersonation and ensure the security of exam data?
- ii. How does the mechanism address privacy concerns, especially when dealing with sensitive information such as biometric data or surveillance?

H. Future Directions and Recommendations:

- i. What are your insights into future developments or enhancements for secure impersonation detection mechanisms in traditional in-class exams?
- ii. Are there emerging technologies or research areas that hold promise?
- iii. Based on your research and design experience, what recommendations or best practices would you offer to educational institutions interested in implementing such a mechanism prototype?
- iv. Are there any critical factors they should consider during the design and deployment?
- v. In your opinion, how does the design of a impersonation detection mechanism enhance the integrity of traditional in-class exams, and what benefits does it bring to educational institutions and students?

I. User Experience and Integration:

- i. How user-friendly is the mechanism for both educators and students? Are there considerations to minimize disruptions during the exam process?
- ii. Can you describe how the mechanism integrates into existing examination processes within traditional classrooms? Were there any challenges or considerations during this integration?

J. Operational Challenges and Solutions:

- i. Were there any challenges or obstacles encountered during the implementation and use of the secure impersonation detection mechanism in traditional in-class exams?
- ii. How were these challenges addressed or mitigated? Are there specific strategies or solutions that were effective?

K. Evaluation Results and Performance Metrics:

- i. How was the effectiveness of the mechanism tested and evaluated? Were specific testing protocols or scenarios used?
- ii. What were the primary performance metrics used to assess the mechanism's effectiveness, and what were the results or findings?

L. Comparison to Existing Methods:

How does the mechanism for detecting impersonations compare to existing methods or practices in terms of accuracy and efficiency?

M. Recommendations and Future Directions:

- i. Based on your evaluation, what recommendations or suggestions would you offer to enhance the mechanism for impersonation detection?
- ii. Are there any areas where the mechanism could be improved or refined?

- iii. What are your insights into potential future developments or enhancements for developed impersonation detection mechanism in traditional in-class exams?

N. Recommendations: In your opinion, how does the evaluated mechanism for detecting impersonations contribute to the integrity of traditional in-class exams, and what benefits does it bring to educational institutions and students?

3 (b) A Survey Questionnaire for collection vies from respondents.

“IMPROVED MECHANISM FOR DETECTING EXAMINATIONS IMPERSONATIONS IN PUBLIC HIGHER LEARNING INSTITUTIONS. CASE OF THE MWALIMU NYERERE MEMORIAL ACADEMY”

A: INTRODUCTION

Thank you for agreeing to take this survey. The survey is being done by Domition, Jasson Lwangisa, a student undertaking a Master’s of Science in Computer Science at the Open University of Tanzania (OUT). The purpose of the survey is to collect opinions from Academic staff, and students who utilizes various methods and mechanisms to authenticate the identity of students so as to check students’ eligibility to seating for a particular exam and who handle various examination illegalities including impersonation fraud. The information supplied will facilitate a study which focuses at designing an improved mechanism for detecting impersonation in traditional-in-class exams context consequently will facilitate the process of identifying impersonators; Informing policy makers in Higher learning institutions on the need to involve ICT in addressing impersonations and it will add knowledge to the already known strategies for detecting impersonations, the result

will influence system developers (programmers) to implementing the recommended impersonation detection mechanism that will consequently solve impersonation frauds experienced by the Tanzania Public higher education institutions and affecting the quality of education and reputation of these institution.

All of the answers you provide in this survey will be kept confidential. No identifying information will be disclosed to third party rather than the intended purpose. The survey data will be reported in a summary fashion only and will not identify any individual person.

This survey will take about 20 minutes to complete.

Questionnaire for objective No. 2: Developing an improved mechanism for detecting impersonations in the context of traditional-in-class examinations.

PARTICIPANTS: Academic Staff

Section 1: Demographic Information

QUESTIONNAIRE

NO.....001

Tick the most correct one

1.1 Sex: MALE []

FEMALE []

1.2 Institute: OUT []

MNMA []

1.3 Age:

Between 18 and 25	Between 26 and 33	Between 34 and 41	Between 42 and 49	Between 50 and 57	Between 58 and 65	Above 66

1.4 Education level:

Bachelor Degree	Postgraduate Diploma	Master's Degree	Doctor of Philosophy (PhD)	Professor

1.5 Work experience (in year(s)): put tick where applicable.

1-2	3-5	6-10	11-15	16- 20	21-25	26-30	31-40	41-50

Section 2: Impersonation Awareness (Tick the appropriate)

S/N	QUESTION	YES	NO
2.1	Are you aware of the concept of impersonation in the context of traditional in-class examinations?		
2.2	Have you ever encountered or heard of cases of impersonation in examinations?		
2.3	Do you believe that impersonation is a serious issue in traditional in-class examinations?		

Section 4: Developing an improved mechanism for detecting impersonation in traditional classrooms.

4.1. Should educational institutions invest in improving mechanisms for detecting impersonations in traditional in-class examinations? (Tick the appropriate)

Strongly Agree ()

Agree ()

Neutral ()

Disagree ()

Strongly Disagree ()

4.2. What features or aspects do you think an improved mechanism for detecting impersonation should possess?

.....

Section 5: Technology Adoption

5.1. Would you be comfortable with the use of technology, such as facial recognition or biometrics, for impersonation detection in examinations? (Tick the appropriate)

5.2 5.1. Would you be comfortable with the use of technology, such as mobile application for impersonation detection in traditional-in exams examinations? (Tick the appropriate)

Yes ()

No ()

Not Sure ()

5.2. What concerns or reservations do you have about the use of technology for impersonation detection?

.....

5.3 What are the prominent traditional-in-class impersonation detection technologies/mechanism do you know?

.....

Section 6: Personal Experience

6.1. Have you ever been wrongly accused of impersonation during an examination? (Tick the appropriate)

Yes ()

No ()

6.2. If yes, please briefly describe your experience and the outcome:

.....

Section 7: Additional Comments

7.1. Please provide any additional comments, suggestions, or insights you have regarding the topic of detecting impersonations in traditional in-class examinations.

(Open-ended)

.....

Section 8: Demographics

8.1. Which country are you currently residing in?

8.2. Are you a student, educator, or another stakeholder in the education sector?

.....

8.3. How frequently do you participate in or administer traditional in-class examinations? (Tick the appropriate)

Frequently ()

Less Frequently ()

More frequently ()

Not at all ()

THANK YOU FOR PARTICIPATING IN THIS QUESTIONNAIRE. YOUR
INPUT IS VALUABLE TO OUR RESEARCH EFFORTS.

QUESTIONNAIRE FOR SPECIFIC OBJECTIVE 3

Questionnaire for Specific Objective 3: Evaluating the developed improved mechanism for detecting impersonations in the context of traditional-in-class examinations.

Participants: ICT expert/staff, students and Academic Staff

Section 1: Participant Information

1.1. Name (Optional):

1.2. Age:

1.3. Gender:

1.4. Educational Background:

1.5. Current Role in Education (e.g., Student, Educator, Administrator):

Section 2: Impersonation Awareness

2.1. Are you aware of the concept of impersonation in the context of traditional in-class examinations? (Tick the appropriate)

Yes ()

No ()

2.2. Have you ever encountered or heard of cases of impersonation in examinations?

(Tick the appropriate)

Yes ()

No ()

Section 3: Familiarity with impersonation detection mechanism

3.1. Are you familiar with the mechanism for detecting impersonations in traditional in-class examinations being evaluated in this study?

Yes ()

No ()

3.2. If yes, please briefly describe your understanding of this framework:

.....

Section 4: Evaluation of the developed impersonation detection mechanism

4.1. In your opinion, how effective is the impersonation detection mechanism for detecting impersonations in traditional in-class examinations? Tick the appropriate)

Very Effective ()

Somewhat Effective ()

Not Effective ()

Not Sure ()

4.2. Have you personally used or experienced the implementation of this mechanism in an educational setting?

Yes ()

No ()

4.3. If yes, please describe your experience and any observations regarding the mechanism's effectiveness:

.....

Section 5: Components of an impersonation detection mechanism

5.1. Please rate the following components of the **impersonation detection mechanism** on their importance for detecting impersonations, with 1 being "Not Important" and 5 being "Very Important":

Authentication methods (e.g., facial recognition, biometrics) ()

Behavior analysis (e.g., keystroke dynamics, eye movement) ()

Monitoring and surveillance tools ()

Data analytics and machine learning algorithms ()

Reporting and alert mechanisms ()

User privacy and data security considerations ()

5.2. Are there any additional components or features you believe should be included in the impersonation detection mechanism for improved impersonation detection?

(Open-ended)

.....

Section 6: impersonation detection mechanism Usability

6.1. How user-friendly do you find the impersonation detection mechanism?

Very User-Friendly ()

Somewhat User-Friendly ()

Not User-Friendly ()

Not Sure ()

.....

Section 7: Evaluation of Outcomes

7.1. Have you observed any positive outcomes or benefits resulting from the implementation of this mechanism? (e.g., reduced impersonation cases, improved exam integrity)

7.2. Have there been any challenges or negative consequences associated with the use of this mechanism?

THANK YOU FOR PARTICIPATING IN THIS QUESTIONNAIRE. YOUR INSIGHTS AND FEEDBACK ARE VALUABLE FOR THE EVALUATION OF THE IMPROVED MECHANISM FOR DETECTING IMPERSONATIONS IN TRADITIONAL IN-CLASS EXAMINATIONS.

3 (c) A Questionnaire For Gathering Students' Responses (In Kiswahili)

Utafiti Juu Ya Kuboresha Namna Ya Kukagua Wanafunzi Kabla Ya Kuingia

Kwenye Vyumba Vya Mitihani

WAHUSIKA

Wahusika ni wanafunzi waliochaguliwa kuwakilisha wanafunzi wote katika Chuo cha kumbukumbubya mwalimu Nyerere.

UTANGULIZI

Tafadhali tusaidie kujibu maswali haya kwa ajili ya utafiti unaofanyika katika vyuo vya elimu ya Juu Tanzania ili kuboresha njia za ukaguzi wakati wa kuingia kwenye vyumba vya mitihani. Maelezo unayoyotoa ni siri na hayatatumika kinyume na lengo la utafiti huu. hakuna taarifa za utambuzi zitakazo sambazwa kwa namna yoyote. taarifa zako ni siri. Nashukururu kwa kushiri katika utafiti huu.

SEHEMU YA KWANZA: MAONI YA JUMLA

1. Je, uliwai kushuhudia mwanafunzi anayesaidia kufanya mtihani/anamfanyia mwenzake mtihani anapambana na Msimamizi wa mtihani? Mfano kutoa lugha kali, kupiga au kutishia kumpiga msimamizi wa mtihani au matukio mengine yenye kuleta fujo kama hayo?
 - A. NDIYO.....
 - B. HAPAN.....
2. Je walinzi wana nafasi yoyote ya kiusalama wakati kipindi cha Mitihani kikiendelea hasa katika mazingira ya Chuo?
 - A. NDIYO.....
 - B. HAPAN.....

3. Kama jibu la juu ni hapana toa sababu

.....

4. Taja umri wako

SEHEMU YA PILI

MTAZAMO WA WANAFUNZI KUHUSU KUSAIDIANA KUFANYA
 MITIHANI NA MWENENDO WA KUSAIDIANA KUFANYIANA MITIHANI
 CHUONI. TANGU MWAKA 2021/2022 HADI MWAKA WA 2023/2024

5. Programu unayosoma.....

6. Mwaka unao soma.....

7. Kwa maoni yako, je ni vema mwanafuzi mmoja kumsaidia mwanafunzi
 mwenzake kufanya mtihani kwa niaba yake (yaani kumfanyia mtihani) kama
 sehemu ya kujipatia baraka kutoka kwa Mungu au faida nyingine kama vile
 kupata ada ya kulipia masomo yake au kodi ya pango?

- A. NINAKBALI SANA

- B. NINAKUBALI

- C. SKUBALI

- D. SIKUBALI KABISA

- E. SINA MAONI

8. Je, mwanafunzi au mtu aliyekuwa anamfanyia mtihani alikuwa nani?

- A. MWANAFUNZI

- B. SIYO MWANAFUNZI

- C. SIKUMTAMBUA

- D. SIJAWAI KUONA

9. Kama jibu la juu ni Ndiyo ilikuwa mwaka gani?

.....

10. Je mwanafunzi aliyekuwa anamsaidia mwenzake kufanya mtihani aligundurika na wasimamizi wa mtihani kwamba anamsaidia mwenzake?

- A. NDIYO
- B. HAPANA
- C. SIJUI
- D. SIJAWAI KUONA

11. Je wewe binafsi uliwai kumsaidia mwenzako kufanya mtihani?

- A. NDIYO
- B. HAPANA

12. Kama jibu ni ndiyo, ulitumia njia gani?

- A. KITAMBULISHO CHANGU CHA CHUO
- B. NILIAZIA KITAMBULISHO
- C. NILIFOJI KITAMBULISHO
- D. NYINGINE
- E. SIJAWAI KUSHIRIKI

13. Je, ulikamatwa?

- A. NDIYO
- B. HAPANA
- C. SIJAWAI KUSHIRIKI

14. Kama hukukamatwa, Unahisi ni kwa nini hukukamatwa?

.....

MWHISHO: HASANTE KWA KUSHIRIKI KUJAZA MASWALI YOTE.

TAARIFA ULIZOTOA NI SIRI NA ZITATUMIKA KWA AJILI YA KUFANIKISHA UTAFITI HUU TU, HAKUNA TAARIFA BINAFSI ZITAKAZO TOLEWA KWA MTU YEYOTE. PALE ITAKAPO BIDI JINA LA UONGO (SYNONYMAS NAME) LITATUMIKA KUTOLEA UFAFANUZI JAMBO FULANI.

Appendix 4: Sample Dynamic Challenging Questions Generated from the NLP

Model for each Test Case (Abuse Case Scenario)

Test Case (TC)/Abuse Case Scenario	DCQS	Number of Correct Responses	Percentage of Correct Responses	Remarks
TC1	What is your Advanced School Region?	2	50	Impersonations case
	What is Your Next of Keen Region?			
	When did you graduate College?			
	What is your Last Name?			
TC2	What is your Home District?	1	25	Impersonations Case
	What is your Next of Keen Relationship?			
	When did you Complete Primary School?			
	What is Your Next of Keen Relationship?			
TC3	When did you Complete Your Primary School?	2	50	Impersonations case
	What is your Last Name?			
	What is your Next of Keen Relationship?			
	What is your Next of Keen Name?			
TC4	When did you Graduate College?	0	0	Impersonations Case

	What is Your Secondary School Region?			
	When did you Complete Secondary School?			
	What is your Secondary School Name?			
TC 5	What is your Next of Keen Name?	1	25	Impersonations case
	What is your Date of Birth?			
	What is your Primary School Region?			
	What is your Primary School Region?			
TC6	What is your Home Region?	0	0	Impersonations case
	What is your Primary School Region?			
	What is your Next of Kin Region?			
	What is your Date of Birth?			
TC 7	What is your Primary School Region?			
	What is your Advanced School Region?	1	25	Impersonations case
	What is your date of Birth?			
	What is your Next of Keen			

	Region?			
TC8	When did you Complete Primary School?	2	50	Impersonations case
	What is your Next of Kin Relationship?			
	What is your Primary School Region?			
	What is your Date of Birth?			

Appendix 5: Selected System's User Interfaces

5 (a) Course Registration Interface

S.A.S / **Manage Course**

Department From

Course Name

Course Short Name

Course Level

Duration / Period

[Submit Course](#)

© 2024 , Developed ❤️ by Mr. Jasson

5 (b) System Administration Panel

S - A - S

- [Dashboard](#)
- [Departments](#)
- [Courses](#)
- [Modules](#)
- [Venues](#)
- [Students](#)
- [Invigilators](#)
- [Exams](#)
- [Reports](#)

ication System , You have alot todo in Here!

Students 15

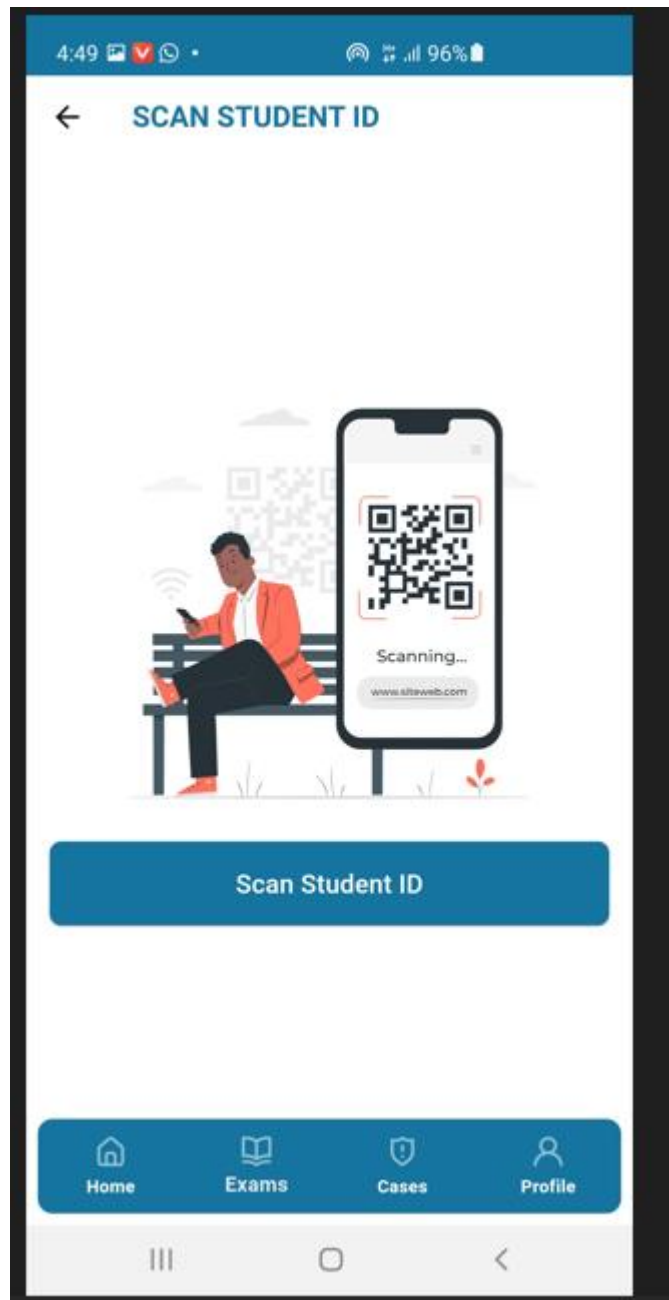
Invigilators 10

Impersonation 0

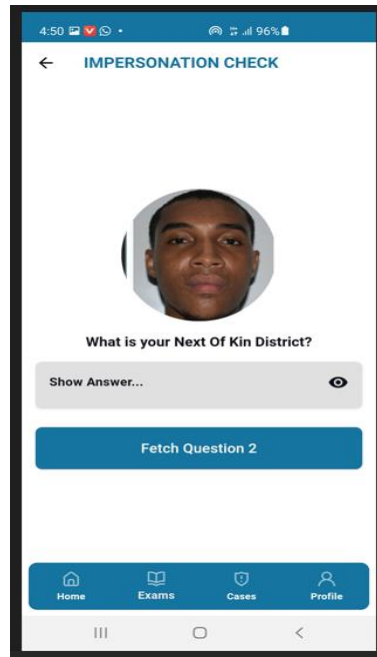
Attendance 0

Exams 9

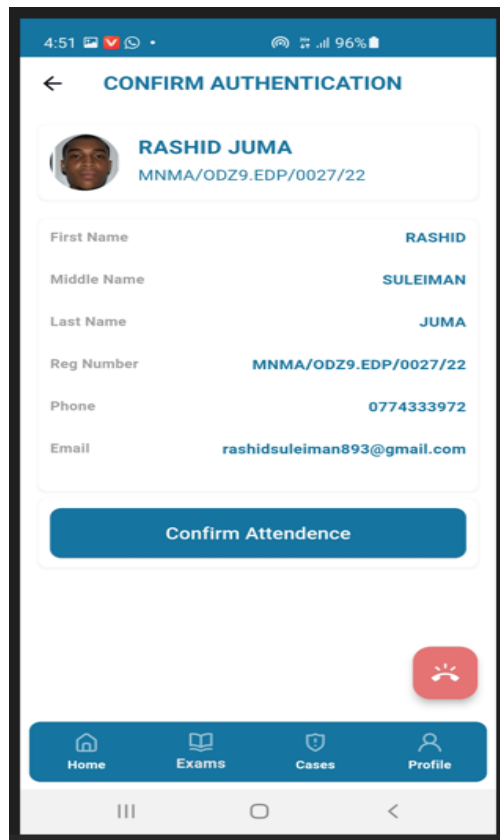
Modules 20

5 (c) An Interface for Scanning Student's IDQR code

5 (d) An Interface for Displaying DCQBSP along their Answers



5 (e) An Interface for Confirming Student Attendance or Impersonations.



5 (f) An Interface for Confirming Exam Eligibility/Reporting impersonations

The image shows a mobile application interface for reporting exam impersonations. At the top, a red banner displays a 'Fail!' message: 'Student is not Allowed to sit for this Exam! Caught Student :'. Below this, there are input fields for 'Registration Number as in Sacnned ID', 'Fullname', and 'Phone Number'. A character count '0/10' is visible next to the phone number field. A larger text area is labeled 'Comment'. Below the main form, there are two sections for witnesses. The 'First Witnessed Student :' section has fields for 'Registration Number' and 'Comment'. The 'Second Witnessed Student:' section is partially visible. At the bottom, a blue navigation bar contains icons and labels for 'Home', 'Exams', 'Cases', and 'Profile'. The very bottom of the screen shows the standard Android navigation bar with three icons.

4:52 95%

Fail!
Student is not Allowed to sit for this Exam!
Caught Student :

Registration Number as in Sacnned ID

Fullname

Phone Number 0/10

Comment

First Witnessed Student :

Registration Number

Comment

Second Witnessed Student:

Home Exams Cases Profile

***Appendix 6: The Actual Implementation of Core Parts of the Proposed
Impersonations Detection System (Coding)***

6 (a) Codes for scanning student' QR code

```
// getStudentsPhoto

public function getStudentsPhoto(Request $request)
{
    $request->validate([
        'regno' => 'required',
        'examination_id' => 'required',
    ]);

    try {
        $user = User::where('regno', $request->regno)->first();

        if (!$user) {
            return response()->json([
                'status' => false,
                'message' => 'Invalid ID QR Code!'
            ]);
        }

        $check = Examinationstudent::where('user_id', $user->id)-
>where('examination_id', $request->examination_id)->first();

        if (!$check) {
```

```

        return response()->json([
            'status' => false,
            'message' => 'Student is not Allowed to sit for this Examination!'
        ]);
    }

    $student = Student::select('photo')->where('user_id', $user->id)->first();

    return response()->json([
        'status' => true,
        'photo' => $student->photo,
        'victimID' => $user->id,
    ]);
} catch (\Throwable $th) {
    return response()->json([
        'status' => false,
        'message' => 'Problem Resulted!',
        'errors' => $th->getMessage()
    ]);
}
}

```

6 (b) Codes for Generating Dynamic Challenging Questions (DCQNs) based on Student Profile.

```

1.      // scanIdCard
2.      public function generateQuestions(Request $request)
3.      {
4.          // validate user_id
5.          $request->validate([
6.              'user_id' => 'required',
7.          ]);
8.
9.          try {
10.             $user = User::findOrFail($request->user_id);
11.
12.             // find student
13.             $student = Student::where('user_id', $user->id)->first();
14.
15.             // Get the column names of the user and student tables
16.             $userColumns = Schema::getColumnListing('users');
17.             $studentColumns = Schema::getColumnListing('students');
18.
19.             // Define columns to exclude
20.             $excludeUserColumns = $this->excludeUserColumns();
21.
22.             $excludeStudentColumns = $this->excludeStudentColumns();
23.
24.             // Remove the excluded columns from the lists
25.             $userColumns = array_diff($userColumns, $excludeUserColumns);
26.             $studentColumns = array_diff($studentColumns,
27.             $excludeStudentColumns);
28.             // Merge the remaining column names

```



```

29.         $columns = array_merge($userColumns, $studentColumns);
30.
31.         // Retrieve the list of already asked questions for the user from session
or database
32.         $askedQuestions = session()->get('asked_questions_' . $user->id, []);
33.
34.         // If all columns have been asked, reset the asked questions list
35.         if (count($askedQuestions) === count($columns)) {
36.             $askedQuestions = [];
37.         }
38.
39.         // Filter out columns that have already been asked
40.         $remainingColumns = array_diff($columns, $askedQuestions);
41.
42.         // If there are remaining columns, pick one randomly
43.         if (count($remainingColumns) > 0) {
44.             $selectedColumn = array_rand($remainingColumns);
45.             $columnName = $remainingColumns[$selectedColumn];
46.             $question = $this->generateQuestion($columnName); // Generate
question based on column name
47.             $askedQuestions[] = $columnName;
48.
49.             // Store the updated list of asked columns in session or database
50.             session()->put('asked_questions_' . $user->id, $askedQuestions);
51.
52.             return response()->json([
53.                 'question' => $question,
54.                 'response' => $student->{$columnName} ?? $user-
>{$columnName} ?? 'N/A',
55.             ]);
56.         } else {
57.             // If all questions have been asked, return a message indicating so

```

```

58.         return response()->json([
59.             'message' => 'All questions have been asked.',
60.         ]);
61.     }
62. } catch (\Throwable $th) {
63.     return response()->json([
64.         'status' => false,
65.         'message' => 'Problem Resulted!',
66.         'errors' => $th->getMessage()
67.     ]);
68. }
69. }
70.
71. /**
72.  * Generate a question based on the column name.
73.  *
74.  * @param string $columnName
75.  * @return string
76.  */
77. // Generate a question based on the column name.
78. private function generateQuestion(string $columnName): string
79. {
80.     // Replace underscores with spaces and capitalize the words
81.     $formattedColumnName = ucwords(str_replace('_', ' ', $columnName));
82.
83.     // Determine the question structure based on column name
84.     $questionPrefix = $this->getQuestionPrefix($columnName);
85.
86.     // Construct the question
87.     return "$questionPrefix $formattedColumnName?";
88. }
89. /**

```

```

90.      * Get the question prefix based on the column name.
91.      *
92.      * @param string $columnName
93.      * @return string
94.      */
95.      private function getQuestionPrefix(string $columnName): string
96.      {
97.          // Determine the appropriate question prefix based on the column name
98.          $questionPrefix = 'What is your'; // Default prefix
99.
100.         // Add more conditions for different question prefixes
101.         if (str_contains($columnName, 'complete_primary_school') ||
str_contains($columnName, 'complete_secondary_school') ||
str_contains($columnName, 'complete_advanced_school') ||
str_contains($columnName, 'graduate_collage')) {
102.             $questionPrefix = 'When did you';
103.         }
104.
105.         return $questionPrefix;
106.     }
107.
108.     // excludeUserColumns
109.     public function excludeUserColumns()
110.     {
111.         return ['id', 'created_at', 'updated_at', 'password', 'status', 'role_id',
'firstname', 'middlename', 'regno', 'phone', 'email'];
112.     }
113.
114.     // getStudentsColumns
115.     public function excludeStudentColumns()
116.     {

```

```

117.     return [
118.         'id',
119.         'course_id',
120.         'user_id',
121.         'gender',
122.         'photo',
123.         'year',
124.         'status',
125.         'created_at',
126.         'updated_at',
127.     ];
128. }

```

6 (c) Codes for Confirming Students Attendance

```

//takeAttendance

public function takeAttendance(Request $request)
{
    $request->validate([
        'user_id' => 'required',
        'examination_id' => 'required',
    ]);
    try {
        // check if attendance already taken
        $check = Examinationstudent::where('user_id', $request->user_id)-
>where('examination_id', $request->examination_id)
        ->where('status', 1)
        ->first();

        if ($check) {
            return response()->json([
                'status' => false,

```

```

        'message' => 'Attendance Already Taken!'
    );
}

$check = Examinationstudent::where('user_id', $request->user_id)-
>where('examination_id', $request->examination_id)
->first();

$check->status = 1;
$check->save();

return response()->json([
    'status' => true,
    'message' => 'Attendance Taken Successfully!'
]);
} catch (\Throwable $th) {
    return response()->json([
        'status' => false,
        'message' => 'Problem Resulted!',
        'errors' => $th->getMessage()
    ]);
}
}

```

6 (d) Codes for Confirming and Reporting Impersonations.

```

//reportImpersonations

public function reportImpersonations(Request $request)
{
    $request->validate([
        'user_id' => 'required',
        'id_caught' => 'required',
        'theft_phone' => 'required',

```

```

        'theft_fullname' => 'required',

        'theft_comment' => 'required',

        'photo' => 'required',

        'examination_id' => 'required',

        'invigilator_comment' => 'required',

        'witness1_regno' => 'required',

        'witness1_comment' => 'required',

        'witness2_regno' => 'required',

        'witness2_comment' => 'required',

    ]);

    if(!$request->hasFile('photo')){
        return response()->json([
            'status' => false,
            'message' => 'Photo is required!'
        ]);
    }

    try {
        // check if impersonations already reported
        $check = Impersonations::where('user_id', $request->user_id)
            ->where('id_caught', $request->id_caught)
            ->where('examination_id', $request->examination_id)->first();

        if ($check) {
            return response()->json([
                'status' => false,
                'message' => 'Impersonations Already Reported!'
            ]);
        }
    }

```

```

// upload photo
$imageName = time() . '.' . $request->file('photo')->extension();
$request->file('photo')->storeAs('public/impersonations', $imageName);
$imagePath = 'storage/impersonations/' . $imageName;

$impersonations = new Impersonations();
$impersonations->user_id = $request->user_id;
$impersonations->id_caught = $request->id_caught;
$impersonations->theft_phone = $request->theft_phone;
$impersonations->theft_fullname = $request->theft_fullname;
$impersonations->theft_comment = $request->theft_comment;
$impersonations->photo = $imagePath;
$impersonations->examination_id = $request->examination_id;
$impersonations->invigilator_comment = $request->invigilator_comment;
$impersonations->witness1_regno = $request->witness1_regno;
$impersonations->witness1_comment = $request->witness1_comment;
$impersonations->witness2_regno = $request->witness2_regno;
$impersonations->witness2_comment = $request->witness2_comment;
$impersonations->save();

$message = "Kuna Uharifu chumba cha mtihani ( " .
    $impersonations->examination->venue->venue . " ) fika haraka!.";
// $phone = "0759503853";
$phone = "0743196599";

if ($impersonations) {
    Helper::sendMessage($message, $phone);
}

return response()->json([
    'status' => true,
    'message' => 'Impersonations Reported Successfully!'
]);

```

```

    } catch (\Throwable $th) {
        return response()->json([
            'status' => false,
            'message' => 'Problem Resulted!',
            'errors' => $th->getMessage()
        ]);
    }
}

```

6 (e) Implementing user Login Page (Administrator page and other system users) on the Web application.

```

//Login users here

public function authenticate(Request $request)
{
    $request->validate([
        'regno' => ['required', 'string'],
        'password' => ['required', 'string'],
    ]);

    $check = User::where('regno', $request->regno)->first();

    if ($check && Hash::check(request('password'), $check->password)) {
        Auth::login($check);

        return redirect('/home');
    } else {
        session()->flash('error', 'Wrong Reg Number or password');

        return redirect('/');
    }

    session()->flash('error', 'Wrong Reg Number or password');
}

```



```

    redirect('/');
}

```

6 (f) Implementing user login Page (Administrator page and other system users) on the Mobile Application.

```

//loginUser
public function loginUser(Request $request)
{
    $validator = Validator::make($request->all(), [
        'regno' => 'required',
        'password' => 'required'
    ]);
    try {
        $check = User::where('regno', $request->regno)
            ->first();

        if ($check && Hash::check(request('password'), $check->password)) {

            $data = [
                'id' => $check->id,
                'firstname' => $check->firstname,
                'middlename' => $check->middlename,
                'lastname' => $check->lastname,
                'regno' => $check->regno,
                'email' => $check->email,
                'phone' => $check->phone,
                'role' => $check->role_id,
            ];

            return response()->json([
                'status' => true,

```

```

        'message' => 'Logged In Successfully!',
        'user' => $data
    });
} else {

    return response()->json([
        'status' => false,
        'message' => 'Wrong Reg Number or Password!',
    ]);
}
} catch (\Throwable $th) {
    return response()->json([
        'status' => false,
        'message' => 'Problem Resulted!',
        'errors' => $th->getMessage()
    ]);
}
}

```

6 (g) Adding New Examination to the Database.

```

// newExamination

public function newExamination(Request $request)
{
    // validate

    $request->validate([

        'module' => 'required',

        'venue' => 'required',

        'examination_date' => 'required',

        'start_time' => 'required',

```

```

        'end_time' => 'required|after:start_time',

        'examination_type' => 'required',

    ]);

    // check if invigilators are selected
    if (empty($request->invigilators)) {

        return redirect()->back()->with('error', 'Please select invigilators');

    }

    // create
    $examination = new Examination();

    $examination->module_id = $request->module;

    $examination->venue_id = $request->venue;

    $examination->examination_date = $request->examination_date;

    $examination->start_time = $request->start_time;

    $examination->end_time = $request->end_time;

    $examination->examination_type = $request->examination_type;

    $examination->save();

    // foreach invigilators
    foreach ($request->invigilators as $invigilator) {

        $invig = new ExaminationInvigilators();

        $invig->user_id = $invigilator;

        $invig->examination_id = $examination->id;

        $invig->save();

    }

```

```

// redirect

return redirect()->route('examinations')->with('success', 'Examination added
successfully');

}

```

6 (h) Codes for Assigning Students to an Examination.

```

// addtoAttendance

public function addToAttendance(Request $request, $examination_id)
{
    // check if one of the student status i 1

    $started_attending = Examinationstudent::where('examination_id',
$examination_id)->where('status', 1)->get();

    if (count($started_attending) > 0) {

        return redirect()->back()->with('error', 'Some students have already started
attending this examination, you can not add more students to this examination');

    }

    // if null

    if (empty($request->attendance)) {

        return redirect()->back()->with('error', 'Please select students to add to
attendance');

    }

    Examinationstudent::where('examination_id', $examination_id)->delete();

    foreach ($request->attendance as $student) {

```

```

        $attend = new Examinationstudent();

        $attend->user_id = $student;

        $attend->examination_id = $examination_id;

        $attend->save();

    }

    return redirect()->back()->with('success', 'Students Added In Examination
successfully');

}

// addAllStudents

public function addALToAttendance($examination_id)

{

    $started_attending = Examinationstudent::where('examination_id',
$examination_id)->where('status', 1)->get();

    if (count($started_attending) > 0) {

        return redirect()->back()->with('error', 'Some students have already started
attending this examination, you can not add more students to this examination');

    }

    // find students for this examination

    $students = Student::select('students.user_id')

        ->where('course_id', Examination::find($examination_id)->module-
>course_id)->where('year', Examination::find($examination_id)->module->year)-
>get();

    // delete all students

    Examinationstudent::where('examination_id', $examination_id)->delete();

```

```

// add all to examinationstudents

foreach ($students as $student) {

    $attend = new Examinationstudent();

    $attend->user_id = $student->user_id;

    $attend->examination_id = $examination_id;

    $attend->save();

}

return redirect()->back()->with('success', 'All Students Added In Examination
successfully');

}

```

6 (i) Codes for Adding Students to the Database (Students Registration).

```

// newStudent

public function newStudent(Request $request)

{

    // validate

    $request->validate([

        'photo' => 'required|image|mimes:jpeg,png,jpg|max:9048',

        'advanced_school_name' => 'nullable',

        'complete_advanced_school' => 'nullable',

        'advanced_school_region' => 'nullable',

        'advanced_school_district' => 'nullable',

        'regno' => 'required|unique:users,regno',

    ]);
}

```

```

$course = Course::find($request->course);

$request->validate([

    'year' => 'required|lte:' . $course->years,

], [

    'year.lte' => 'Student year must be less than Course years ' . $course->years,

]);

// upload photo

$imageName = time() . '.' . $request->file('photo')->extension();

$request->file('photo')->storeAs('public/uploads', $imageName);

$imagePath = 'storage/uploads/' . $imageName;

// user

$user = new User();

$user->firstname = $request->firstname;

$user->middlename = $request->middlename;

$user->lastname = $request->lastname;

$user->regno = $request->regno;

$user->phone = $request->phone;

$user->email = $request->email;

$user->role_id = 3;

$user->password = Hash::make($request->regno);

$user->save();

// student

$student = new Student();

$student->course_id = $request->course;

```

```

$student->user_id = $user->id;

$student->gender = $request->gender;

$student->date_of_birth = $request->date_of_birth;

$student->photo = $imagePath;

$student->home_region = $request->region;

$student->home_district = $request->district;

$student->primary_school_name = $request->primary_school_name;

$student->complete_primary_school = $request->complete_primary_school;

$student->primary_school_region = $request->primary_school_region;

$student->primary_school_district = $request->primary_school_district;

$student->secondary_school_name = $request->secondary_school_name;

$student->complete_secondary_school = $request-
>complete_secondary_school;

$student->secondary_school_region = $request->secondary_school_region;

$student->secondary_school_district = $request->secondary_school_district;

$student->advanced_school_name = $request->advanced_school_name;

$student->complete_advanced_school = $request->complete_advanced_school;

$student->advanced_school_region = $request->advanced_school_region;

$student->advanced_school_district = $request->advanced_school_district;

$student->collage_name = $request->collage_name;

$student->graduate_collage = $request->graduate_collage;

$student->collage_region = $request->collage_region;

$student->collage_district = $request->collage_district;

$student->next_of_kin_relationship = $request->next_of_kin_relationship;

```



```

    $student->next_of_kin_name = $request->next_of_kin_name;
    $student->next_of_kin_region = $request->next_of_kin_region;
    $student->next_of_kin_district = $request->next_of_kin_district;
    $student->year = $request->year;
    $student->save();
    // redirect

    return redirect()->route('students')->with('success', 'New Student added
successfully');
}

```

6 (j) Adding Invigilators to the Database (Invigilators Registration).

```

// newInvigilator

public function newInvigilator(Request $request)
{
    // validate
    $request->validate([
        'regno' => 'required|unique:users,regno',
        'firstname' => 'required',
        'middlename' => 'nullable',
        'lastname' => 'required',
        'phone' => 'required',
        'email' => 'required|email|unique:users,email',
    ]);
    // save user
    $user = new User();
    $user->regno = $request->regno;
    $user->firstname = $request->firstname;
    $user->middlename = $request->middlename;
    $user->lastname = $request->lastname;
    $user->phone = $request->phone;
}

```

```

    $user->email = $request->email;
    $user->role_id = 2;
    $user->password = Hash::make($request->regno);
    $user->save();

    // redirect
    return redirect()->route('invigilators')->with('success', 'Invigilator added
successfully');
}

// goeditInvigilator
public function goeditInvigilator($id)
{
    $invigilator = User::find($id);
    return view('pages.new_invigilator', [
        'invigilator' => $invigilator,
    ]);
}

// updateInvigilator
public function updateInvigilator(Request $request, $id)
{
    // validate
    $request->validate([
        'regno' => 'required|unique:users,regno,' . $id,
        'firstname' => 'required',
        'middlename' => 'nullable',
        'lastname' => 'required',
        'phone' => 'required',
        'email' => 'required|email|unique:users,email,' . $id,
    ]);
    // save user
    $user = User::find($id);

```

```
$user->regno = $request->regno;
$user->firstname = $request->firstname;
$user->middlename = $request->middlename;
$user->lastname = $request->lastname;
$user->phone = $request->phone;
$user->email = $request->email;
$user->role_id = 2;
$user->password = Hash::make($request->phone);
$user->save();
// redirect
return redirect()->route('invigilators')->with('success', 'Invigilator updated
successfully');
}
```

Appendix 7: Research Clearance Letters from the University and research area.



Ref. No OUT/PG202086723

19th June, 2024

Rector,
The Mwalimu Nyerere Memorial Academy (MNMA),
P.O. Box 9193,
DAR ESS SALAAM.

Dear Rector

RE: RESEARCH CLEARANCE FOR MR. JASSON LWANGISA DOMITION REG NO: PG202086723

2. The Open University of Tanzania was established by an Act of Parliament No. 17 of 1992, which became operational on the 1st March 1993 by public notice No.55 in the official Gazette. The Act was however replaced by the Open University of Tanzania Charter of 2005, which became operational on 1st January 2007. In line with the Charter, the Open University of Tanzania mission is to generate and apply knowledge through research.

3. To facilitate and to simplify research process therefore, the act empowers the Vice Chancellor of the Open University of Tanzania to issue research clearance, on behalf of the Government of Tanzania and Tanzania Commission for Science and Technology, to both its staff and students who are doing research in Tanzania. With this brief

background, the purpose of this letter is to introduce to you **Mr. Jasson Lwangisa Domition, Reg.No: PG202086723**), pursuing **Masters of Science in Computer Science (MSc-COMPUTER)**. We here by grant this clearance to conduct a research titled **“Improved Mechanism for Detecting Traditional-In-Class Examinations Impersonations in Public Higher Learning Institutions: A Case of The Mwalimu Nyerere Memorial Academy**. He will collect his data at your institution from 20th June to 30th July 2024.

4. In case you need any further information, kindly do not hesitate to contact the Deputy Vice Chancellor (Academic) of the Open University of Tanzania, P.O.Box 23409, Dar es Salaam. Tel: 022-2-2668820. We lastly thank you in advance for your assumed cooperation and facilitation of this research academic activity.

Yours sincerely,

THE OPEN UNIVERSITY OF TANZANIA



Prof. Gwahula Raphael Kimamala

For: VICE CHANCELLOR

Appendix 8: A manuscript published in the Journal of computer and communications (JCC).

THE UNITED REPUBLIC OF TANZANIA



**THE MWALIMU NYERERE MEMORIAL
ACADEMY**



When replying please mention:

Ref. No. MNMA/PF.256/30

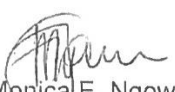
25th July, 2024

Vice Chancellor,
The Open University of Tanzania,
P. O. Box 23409,
DAR ES SALAAM.

**RE: RESEARCH CLEARANCE FOR MR. JASSON LWANGISA DOMITION REG. NO.
PG202086723**

Kindly refer to the heading above and your letter with Ref. No. OUT/PG202086723 dated 19th June, 2024.

2. I am pleased to inform you that, your request for research clearance in respect of your student Jasson Lwangisa Domition is **granted** as requested.
3. During data collection period, the student will be allowed to conduct interview only without involving sensitive information from existing data bases and the collected data have to be used for academic purposes only.
4. Yours Sincerely,


 Monica E. Ngowo
For; RECTOR

THE MWALIMU NYERERE MEMORIAL
 ACADEMY
 P.O. BOX 9193
 DAR-ES-SALAAM

Copy:

- Deputy Rector Academic, Research and Consultancy - MNMA
- Mr. Jasson Lwangisa Domition,
Tutorial Assistant,
The Mwalimu Nyerere Memorial Academy,
P. O. Box 9193,
DAR ES SALAAM.