Scientific Research Publishing

Journal of Computer and Communications, 2024, 12, 160-187
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Improved Mechanism for Detecting Examinations Impersonations in Public Higher Learning Institutions: Case of the Mwalimu Nyerere Memorial Academy (MNMA)

Jasson Lwangisa Domition[1], Rogers Philip Bhalalusesa[2], Selemani Ismail[2]

[1]Department of Leadership and Management Sciences, The Mwalimu Nyerere Memorial Academy, Pemba, Tanzania
[2]Department of Mathematics, Information and Communication Technology, The Open University of Tanzania, Dar es Salaam, Tanzania
Email: jassondomition@gmail.com, bhalaluses@gmail.com, Selemani.ismail@out.ac.tz

How to cite this paper: Domition, J.L., Bhalalusesa, R.P. and Ismail, S. (2024) Improved Mechanism for Detecting Examinations Impersonations in Public Higher Learning Institutions: Case of the Mwalimu Nyerere Memorial Academy (MNMA). *Journal of Computer and Communications*, **12**, 160-187.
https://doi.org/10.4236/jcc.2024.129010

Received: July 17, 2024
Accepted: September 24, 2024
Published: September 27, 2024

Abstract

Currently, most public higher learning institutions in Tanzania rely on traditional in-class examinations, requiring students to register and present identification documents for examinations eligibility verification. This system, however, is prone to impersonations due to security vulnerabilities in current students' verification system. These vulnerabilities include weak authentication, lack of encryption, and inadequate anti-counterfeiting measures. Additionally, advanced printing technologies and online marketplaces which claim to produce convincing fake identification documents make it easy to create convincing fake identity documents. The Improved Mechanism for Detecting Impersonations (IMDIs) system detects impersonations in in-class exams by integrating QR codes and dynamic question generation based on student profiles. It consists of a mobile verification app, built with Flutter and communicating via RESTful APIs, and a web system, developed with Laravel using HTML, CSS, and JavaScript. The two components communicate through APIs, with MySQL managing the database. The mobile app and web server interact to ensure efficient verification and security during examinations. The implemented IMDIs system was validated by a mobile application which is integrated with a QR codes scanner for capturing codes embedded in student Identity Cards and linking them to a dynamic question generation model. The QG model uses natural language processing (NLP) algorithm and Question Generation (QG) techniques to create dynamic profile questions. Results show that the IMDIs system could generate four challenging profile-based questions within two seconds, allowing the verification of 200 students in 33 minutes by one operator. The IMDIs system also tracks exam-eligible students, aiding in exam attendance and integrates with a Short Message Service (SMS) to report

impersonation incidents to a dedicated security officer in real-time. The IMDIs system was tested and found to be 98% secure, 100% convenient, with a 0% false rejection rate and a 2% false acceptance rate, demonstrating its security, reliability, and high performance.

Keywords

Natural Language Processing (NLP) Model, Impersonations Detection, Dynamic Challenging Questions, Traditional-in-Class Examination and Impersonation Detection

1. Introduction

In typical traditional-in-class 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. Impersonation in the other hand is one of the major challenges facing Tanzania public higher learning institutions assessment system where examinations take place in traditional classrooms. Impersonation is 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 [1] and [2].

A study carried out by [3] and a study by [4] indicate that many higher learning institutions prefer traditional-in-class examinations due to difficulty in the identification of students siting for examinations remotely as they lack face-to-face interactions. Under some circumstances, some students invite third parties known as mercenaries to take examinations on their behalf [5]-[7]. Therefore, this study intends to uncover the solution towards detecting impersonations of this kind by formulating an enhanced Natural Language Processing (NLP) Model which applies Questions Generation (QG) technique to improve the mechanism for detecting impersonations. The model reports impersonations proactively to relevant institutional syndicates responsible for taking actions towards academic irregularities of this kind. The study performed an empirical analysis in public higher learning institutions where traditional-in-class examinations take place and where parties engaging in impersonations exist and of course a place where the proposed improved impersonation detection model applies. It was anticipated that developing an enhanced model that utilizes NLP algorithm and its associated technique (QG) could have improved the mechanism for verifying students' examinations (tests and semester examinations) eligibility. Therefore, the designed NLP model (MDIs system) combines two students' identification schemes namely a QR code which stores student registration number and a link to student profile as well as a dynamic profile questions generation algorithm. The scanned student registration number from the QR code is then linked to a centralized student profile system which activates a dynamic challenging questions generation (QG). The QG

technique analyzes student's profile to generate a set of challenging questions based on specific student profile along with their corresponding answers. The generated questions and answers are then presented to a mobile device interface which facilitate student verification process by examination invigilator. Furthermore, the designed model provides a mechanism for confirming student's examinations eligibility and reporting all detected impersonations to the examination office and a dedicated security personnel.

This implementation of an effective solution for detecting impersonations overcomes mercenaries (impersonators) who would always bypass the existing students' identification schemes including a mere QR code embedded in students' identification cards, examinations hall tickets, students' identification cards and other similar students' identification documents.

Therefore, the significance of this study relies on the grounds that current schemes for identifying students are susceptible to manipulations thus can be forged and bypassed to third parties who intend to commit impersonations hence requires a tremendous re-innovation. In addition, fake identity documents have been used to store examinations answers thus violating examination rules and regulations [7]. To discourage students from forging Identity documents and using that loophole to engage in impersonation acts, this study explored the following: The efficiency, security, convenience and usability of the deigned impersonation detection model and whether the shared information between an actual student and mercenaries can facilitate the execution of impersonation in the underlined context.

2. Related Work

Impersonation is a serious examinations cheating behavior and is against the goal of higher education which emphasizes on quality, competence and individual development [1] [8] and [9]. 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, this implies that existing schemes for detecting impersonations have numerous limitations [5] [7] and [10].

A study carried out by [11] in Kenya insists the need to enforcing strategies against the impersonation menace in academic institutions, in that regard, a severe combined moral method to eradicate impersonations from their academic institutions were recommended.

Several studies aimed at preventing impersonations have been conducted for example a study conducted by [12] insisted the use of examination eligibility verification (EEV) and attendance system which relies on a quick response (QR) code that are embedded in students' identification cards and validated by smartphone. The proposed examination eligibility verification system was effective and reliable in verifying student identity over the existed student identification schemes. The EEV system involved two parties namely the invigilator and the 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 the 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 EEV system display eligibility status whenever it finds that a student is registered. In the contrast the system displays not eligible status. Student's ID card is scanned twice to ensure student login and student logout. To achieve system objective, the EEV 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 EEV 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 EEV system was developed by using JavaScript, Cascading Style Sheets, and HTML5 within Microsoft Visual Studio Code, while the server side was implemented by using PHP and MySQL database management system. Chrome web browsers was used to access the system. 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 these students.

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 [13]. It is suggested that supplementing a QR code system with another level of user authentication method is important for enhancing system robustness.

Also [14] implemented a QR code based system as a means of screening examination ineligible students. Therefore the [12] and [14] impersonations detection systems could be modified in terms of capabilities, functionalities and scope so as to add more security, usability features and scanning devices so as to take advantage of the growing smartphone technology.

Nevertheless, other studies suggested different options for curbing impersonations for example, a study conducted by [15] 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 university 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.

Moreover, [16] proposed a Biometric Model (fingerprint) which solves the problem existing in current techniques used for identifying students and detecting impersonators at the Yaba College of Technology in Nigeria. 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 which involves the use of forged biometric object such as plastic fingers in accessing a secured system, this could 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".

In addition, [17] suggests that impersonations in examinations hall can be reduced by verifying students using a bi-modal features of the candidate. This could be an integration of more than one biometric trait to form a bi-model system. However, the bimodal feature suffers similar challenges proven from other biometrics identification systems including poor acceptance rate, forgeries and usability issues.

On the other hand, other studies on impersonations detection suggested the use of barcodes as a suitable mechanism to replacing traditional techniques of identifying students and detecting impersonations. These studies include but not limited to a study by [18]: "Using Barcode to Track Students Attendance and Assets in Higher Education Institutions" and the study by [19]: "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. Findings 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 [19].

In a nutshell, review of some available literatures adds to the understanding that impersonations detection challenge in higher learning institutions is considerably greater than the strategies that are being used to deal with impersonations particularly in Tanzania public higher learning institutions. Looking on the conducted studies on impersonations detection schemes, this phenomenon represents the absence of a holistic mechanism for dealing with impersonations detection not only in Tanzania 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 was of paramount importance [2] [20] and [21].

Focus of the Research

This study focuses mainly on developing an enhanced NLP examinations impersonation detection model based on QG technique that eventually improves the mechanism for filtering out all examinations ineligible candidates and allow only candidates who are eligible to sit for examinations. With this solution, impersonations can be accurately detected and reported to relevant institution authorities. The output of this study is a hybrid model (system) which integrates relevant NLP algorithm and QR code generation technique that dynamically analyses student profile to generate dynamic challenging questions (DCQNs). The proposed system automatically generates dynamic challenging questions based on student profile that a student must answer before he or she can be allowed to access an examination venue. Besides, this implementation facilitates an automatic students' attendance taking solving the problem of manual students' attendance taking existing in current students' verification system.

3. Research Methodology

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 [22] [23]. Also, a mixed research methodology was helpful in assessing the effectiveness of the designed improved impersonations detection Model. In the view of the above, qualitative methods helped to uncover the experiences and perceptions of participants towards the use of the proposed impersonations detection system, while quantitative methods were used to measure the model (system) outcomes and impact. Beside, this study applied an internationally accepted system development methodology known as "prototyping system development methodology" to implement the IMDIs using NLP algorithm and QR code technology. 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 [6]. 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 system 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 system model. It was essential to show how user interact with the implemented impersonations detection mechanism. As a result, prototyping helped both users and researchers validate and evaluate their requirements hence discover requirements that were omitted during requirements

definition stage.

Moreover, to implement the proposed impersonation detection system using NLP algorithm and QR code technology, three software development frameworks were applied. These frameworks provide tools for writing codes that are capable of processing natural language and machine learning models. These frameworks include, flutter framework for implementing a restful mobile app, Laravel Framework for implementing the web part of the system and the MYSQL database management system for managing all database logics and operations. The details for the selected systems development frameworks are presented in the findings and discussion particularly in section 4.7.1 and section 4.7.2.

3.1. Study Area

This study was conducted in Tanzania whereas, The Mwalimu Nyerere Memorial Academy (MNMA) among 48 public higher learning institutions was selected as a case study [24]. The criteria for selecting the study area were based on the availability of information regarding impersonations which was enough to attain the main objective of this study [25]. Also, MNMA is among higher learning institutions in Tanzania which are currently enrolling many students per annum. The current enrollments of the Academy tall to more than Fourteen Thousand (14,000) students (field data). This trend is not equivalent to the growth trend on the number of academic staff available to invigilate examinations, for instance, the Academy had Two Hundred Thirty Five (235) academic staff in the academic year 2023/24 [21]. Yet the Academy has observed an increased impersonation cases in three consecutive years (2020/21 to 2023/24).

3.2. Sample Design

Due to the heterogeneous nature of the specified sample frame, a stratified and random sampling methods were applied to get the required sample size in each stratum. Sample selection method within two strata, namely the academics and students groups respectively involved a simple random sampling method while the rest of the strata namely the ICT staff (experts) and directors/rector for academics involved a purposive sampling technique. The results of sample sizes calculations indicate that 148 academic staff (academics), 388 students; 1 director, 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 [17] [21] [23] and [25]. The Taro Yamane equation ($n = N/1 + Ne^2$); where n=sample size; N = Size of population, e = sampling error (5%) and 95% as the desired confidence level) was invoked to determine sample size for the academic staff and students respectively while a purposive sampling technique was employed in the rest of the strata. In addition, a sample size of 50 students was employed to create a dataset for training and testing the proposed NLP examinations impersonations detection model.

3.3. Research Design

Beside prototyping methodology, design science methods were used to enhance the design process, improving the quality of system design outcomes, addressing specific design-related challenges and evaluating the designed system. To facilitate an evaluation process, an expert survey method was used to gather opinions, insights, and judgments from individuals who possess specialized knowledge, expertise, or experience in the field of education, information and communication technology. These experts possessed expertise in impersonations detection techniques. This was very helpful as it facilitated the development of a very holistic solution based on such expertise and experiences.

4. Findings and Discussion

This section presents findings and discussion from this study.

4.1. Socio-Demographic Attributes of the Respondents

Findings of the study on Technologies' usage among science teachers in federal unity schools in Nigeria which was performed by [5] presents demographic variables and ICT access as predictors of information communication technology usage which is published at http://digitalcommons.unl.edu/libphilprac, Part of the Library and Information Science Commons. These findings show that ICT accessibility (B = 0.431), educational qualification (B = −0.187), teaching experience (B = −0.154), ICT use experience (B = 0.152), and location of ICT access (B = 0.144) as best predictors of ICT use among science teachers. Therefore, 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 system for detecting impersonations in their respective institutions.

4.1.1. Age of Respondents

The study findings on the age indicate that most of the academic staff 129 (99.5%) were of the age between 15 and 55 and most students 353 (98.6%) were of the age between 15 and 45 years which implies that it is the age between youth and elderly people who actively engage in using ICT products such as mobile applications and other mobile device enablers. Thus, these products should enhance mobility, independency and social participation (**Figure 1**).

4.1.2. Education Levels 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 [26]. Results show 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 they had different expertise including computer programming,

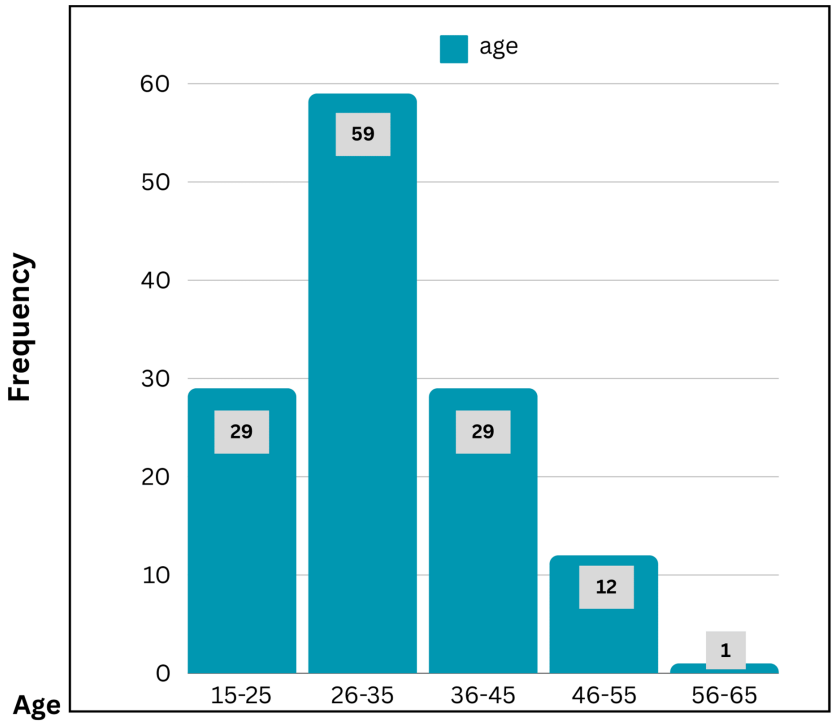

Figure 1. Distribution of respondents by age (field data, 2024).

computer security and software development skills. This implies that the developed model is relevant and have high acceptance rate as it comes from inputs given by educated and experienced staff who are expected to use the designed system.

4.2. Implementation of the Enhanced Natural Language Processing (NLP) Examinations Impersonation Detection Model

Creating a set of dynamic challenging questions to verify the identity of a student and 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 implementation 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; also NLP techniques, especially with models like GPT-4 or BERT, can understand context and generate more natural and relevant questions and that the NLP algorithm can generate highly personalized questions by interpreting complex and varied datasets. However, the NLP algorithm poses some challenges that requires serious considerations such as NLP models can be complex to develop and require significant computational resources (that is 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 details.

4.3. Details of the Developed NLP Examinations Impersonations Detection Model

4.3.1. 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 was collected together to form individual student profile which is trained to the NLP model to generate personalized dynamic challenging questions.

4.3.2. 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).

4.3.3. 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.

Mathematical Representation on the Technique for Generating Dynamic Challenging Questions (QG)

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.

$$D = \{(e_1, v_1), (e_2, v_2), \cdots, (e_n, v_n)\}$$

where e_i represents an entity type (e.g., "Course Name", "Grade", "programme name") and v_i represents the corresponding value (e.g., "Database", "A", "NLP").

Step 2: Named Entity Recognition (NER)

Using NER, we extract entities from D.

$$E = \{e_1, e_2, \cdots, e_n\}$$

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 e_i.

$$T = \{T_1, T_2, \cdots, T_m\}$$

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

$T_1(e_i)$ = "What grade did you receive in" + e_i + "?"

Step 4: Selecting Entities and Generating Questions

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

$$Q_k = T_j(e_i)$$

The set of generated questions Q can be represented as:

$$Q = \{Q_1, Q_2, \cdots, Q_p\}$$

where each Q_k is a question generated by applying a template to an entity.

Step 5: Answer Extraction

For each generated question Q_k, extract the corresponding answer A_k from the dataset D.

Let A be the set of answers:

$$A = \{A_1, A_2, \cdots, A_p\}$$

where each A_k corresponds to the correct answer for question Q_k.

Step 6: Mathematical Representation of the Process

i. Data Extraction:

$$E = NER(D)$$

ii. Template-Based Question Generation:

For each entity $e_i \in E$:

$$Q_k = T_j(e_i)$$

iii. Answer Extraction:

For each generated question Q_k:

$$A_k = D(e_i)$$

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"}

4.3.4. Model Training

The NLP model was trained on Fifty (50) students' dataset and processed data to generate questions. This involved feeding the model with question syntax and

learning how to generate appropriate questions.

4.3.5. 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.

4.3.6. Evaluation

Then the generated challenging questions and answers were evaluated to ensure they are challenging and accurate. The process involved human oversight to make some suggestions based on the generated questions and answers from the designed NLP model.

4.3.7. Dynamic Challenging Questions (DCQNS) Presentations

The DCQNS generated by the system or the model were presented on a mobile device (smart phone) screen showing a question with dynamic placeholders filled in (e.g., "What grade did you receive in Data Structures?") along with its corresponding answer (e.g., "Grade A") (see Figure 2).

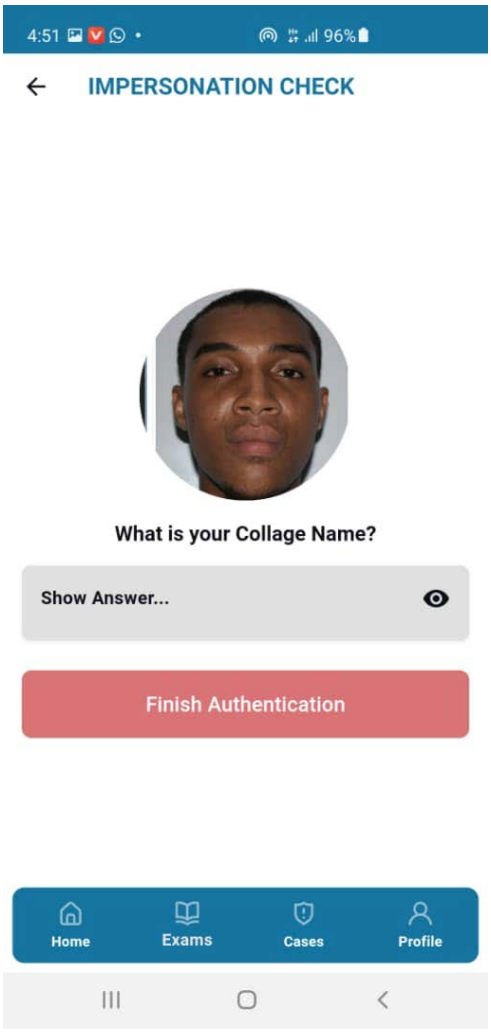

Figure 2. DCQNs and answer presented on a smartphone screen during student authentication.

4.3.8. Impersonation Detection

The system provides a check button indicating to confirm student eligibility or an impersonation and produces a 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 impersonation incidence and take care of security matters (see Figure 3).

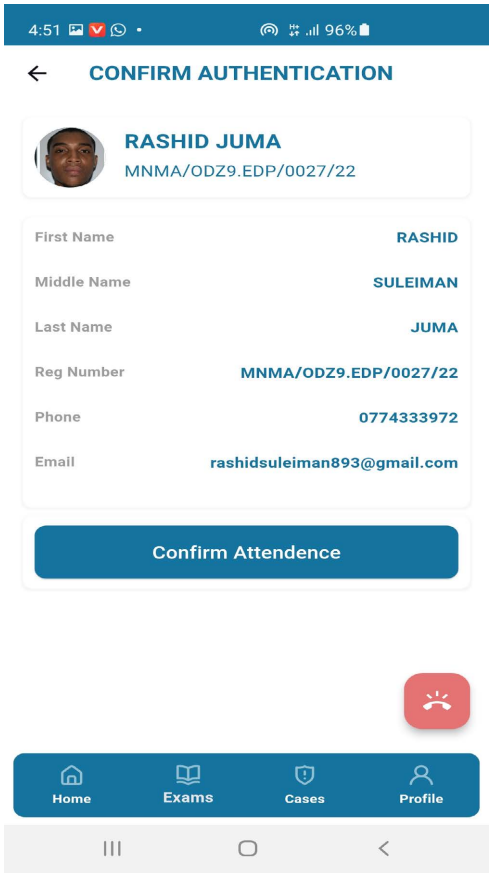

Figure 3. Confirming student attendance or an impersonation case.

The pictorial representation in Figure 4 encapsulates the flow from data collection through to the dynamic challenging questions generation and presentation of questions for student identity verification and impersonation detection exercise in the developed system.

Therefore, the novel contribution of this section is an enhanced NLP model or system which detects examinations impersonations in the context of traditional classrooms. The model integrates QR code technique and dynamic challenging questions generation technique to effectively and timely detect impersonations.

4.4. Proposed System Architecture of the Designed NLP Model (System) for Detecting Examinations Impersonations

The research findings indicate that the proposed improved mechanism for detecting impersonations in traditional-in-class examinations in public higher

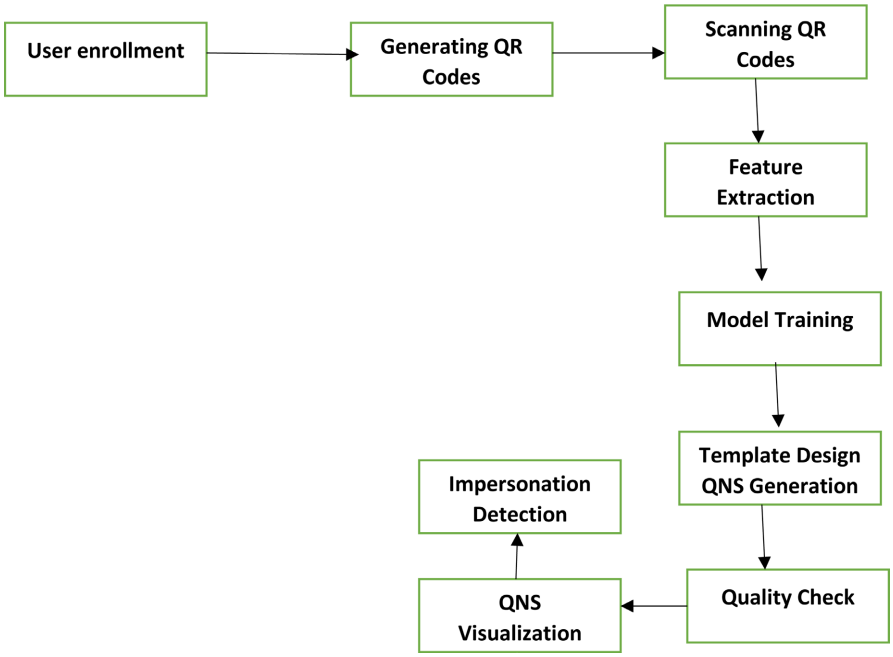

Figure 4. Phases for the proposed system that detects examinations impersonations (Drawn with MS. Word 2013).

learning institutions should include seven major components or modules namely: a user registration module, QR code generation and QR code scanning module, the module for generating dynamic challenging questions based on student's profile, impersonations detection module, attendance taking module, communication module and impersonations reporting module. Users of the proposed system include students, invigilators, examination officers, heads of academic departments, security officers and the system administrator (**Figure 5**).

4.5. Description of the Proposed Improved Impersonation Detection Model (System)

The generation of dynamic challenging questions is activated by a successful scan of a QR code by a smart phone scanner connected to a student verification application. Information for generating dynamic challenging questions is extracted from a student's profile database or dataset which include student's admission information, examinations records, course details, course facilitators' details and parents or gurdians' details. The information is 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 system. 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 a set of four (4) dynamic challenging questions that are created randomly and

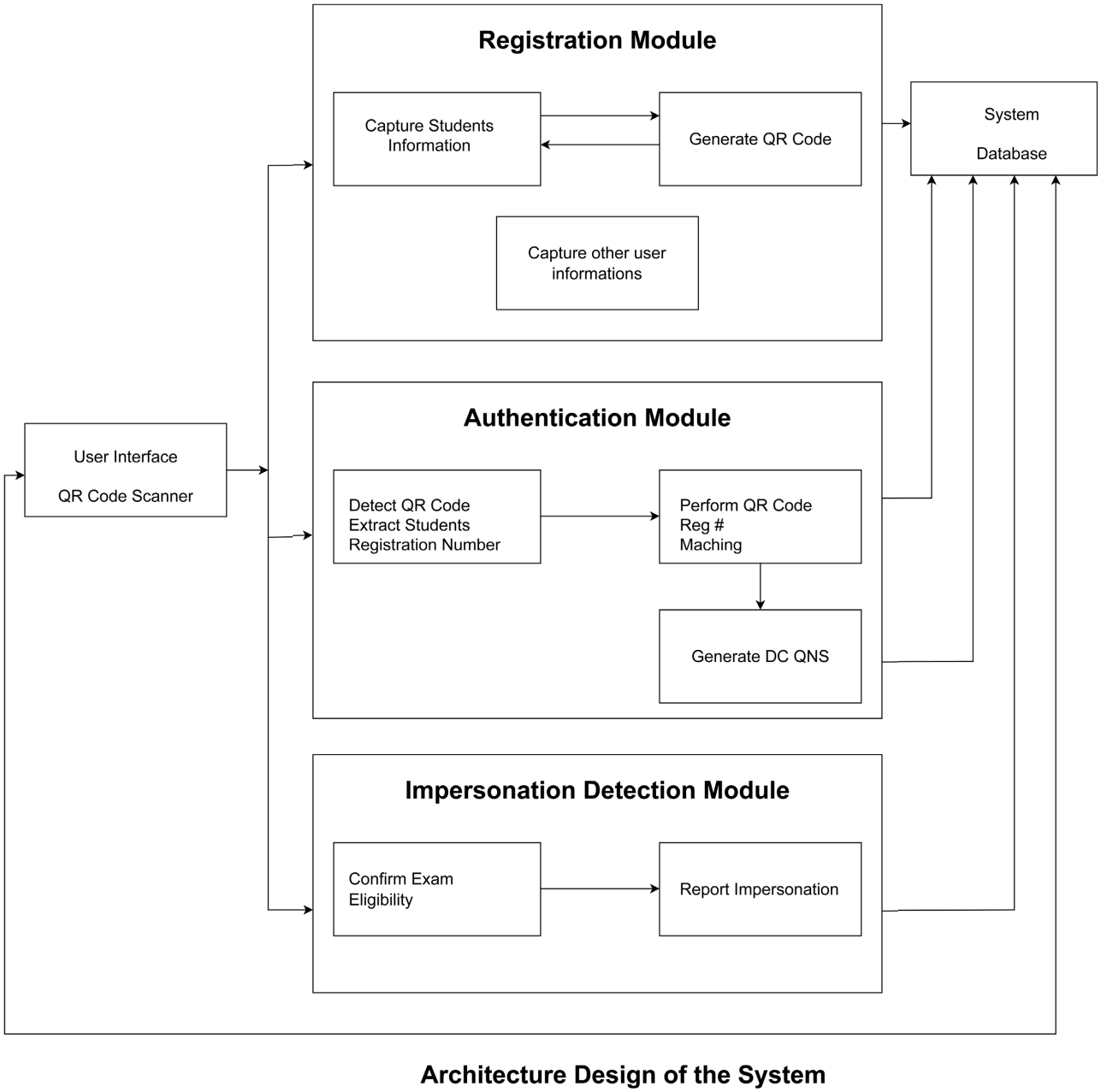

Figure 5. Architectural design of the proposed system (designed in draw.io).

presented to student via smart phone application interface under the supervision of the invigilator. 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 (**Figure 3**). Conversely all confirmed impersonations are reported by the system to the examinations officer who prepares a detailed report and submit it to the office of Academic Research and Consultancy (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.

This study suggests a fixed number of four (4) profile based dynamic challenging questions to remove the possibilities of guessing attacks as discussed later in section 4.8. This implies that when a student appeals to access traditional examination venue, the invigilator should activate the system to automatically generate 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 impersonation in case the scanned QR code in not valid (see **Figure 6** and **Figure 7** for details in section 4.8).

4.6. Major System Operations

This section presents major system operations:

4.6.1. Registration

Student's profile information is captured and stored in the MYSQL database. Moreover, the invigilators details and examinations' information including examinations venue, time and date are also captured and stored in the MYSQL database system.

4.6.2. Generating QR Codes

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

4.6.3. Scanning QR Code

QR code are captured by the smart phone supported camera. A smart phone-based scanner was chosen due to its frequent employment in many mobile applications based on several reasons including convenience, portability, integration, efficiency, accessibility, cost-effectiveness and innovations.

4.6.4. Data Matching

This phase involves comparing the scanned QR code with the existing QR code once the matching is successful students are directed to a series of 4 challenging question.

4.6.5. Generating Dynamic Challenging Questions

Questions are generated based on student's profile associated with the current registration number found in the QR code and displaying them to the smart phone screen along with their corresponding answers. It is the role of the invigilator to observe matching between student's responses and systems generated responses.

4.6.6. Confirming Impersonations

An invigilator system interface provides a provision to confirm student eligibility or report impersonation (**Figure 3**). Every action is reported to relevant intuition

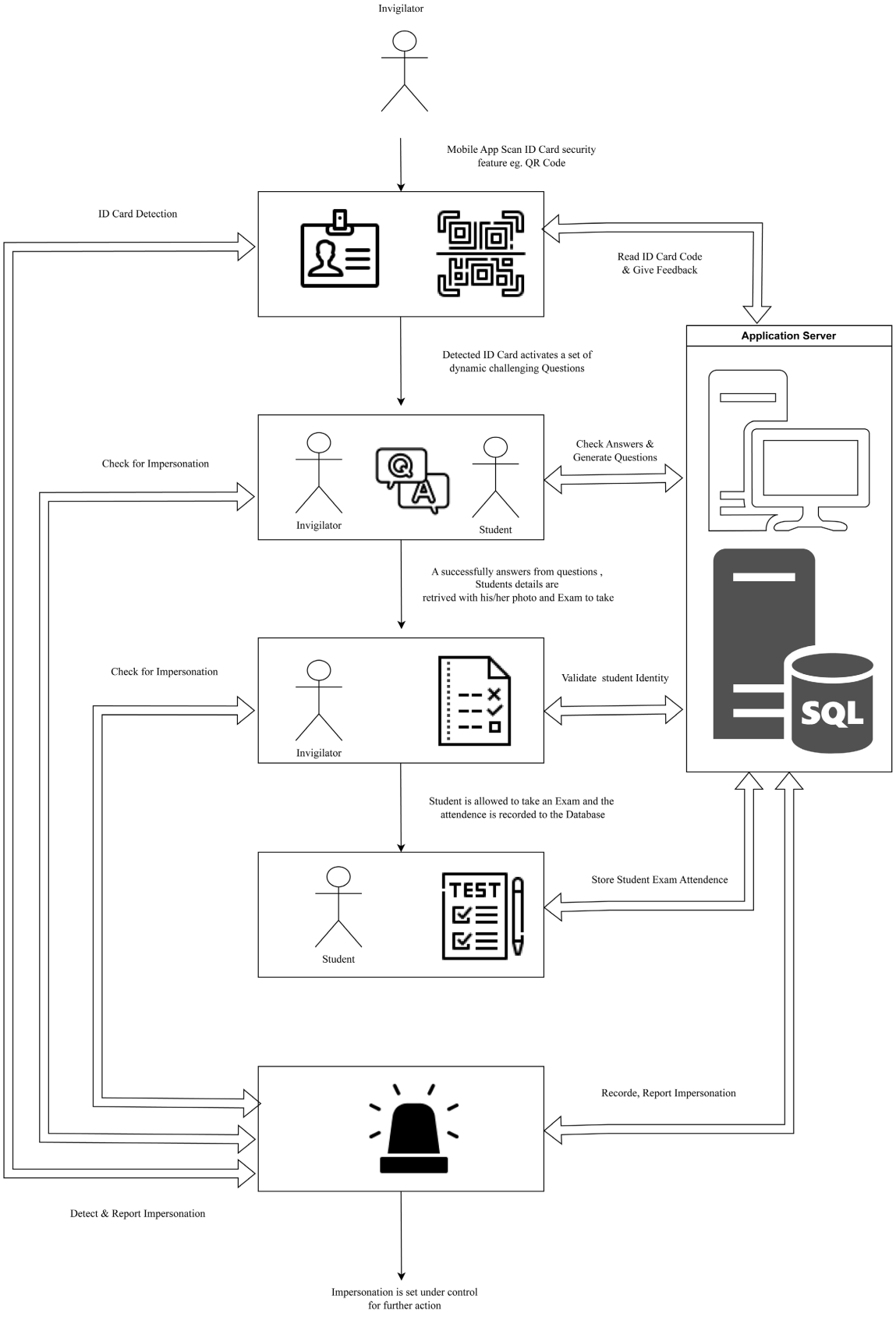

Figure 6. A Conceptual design describing student eligibility verification.

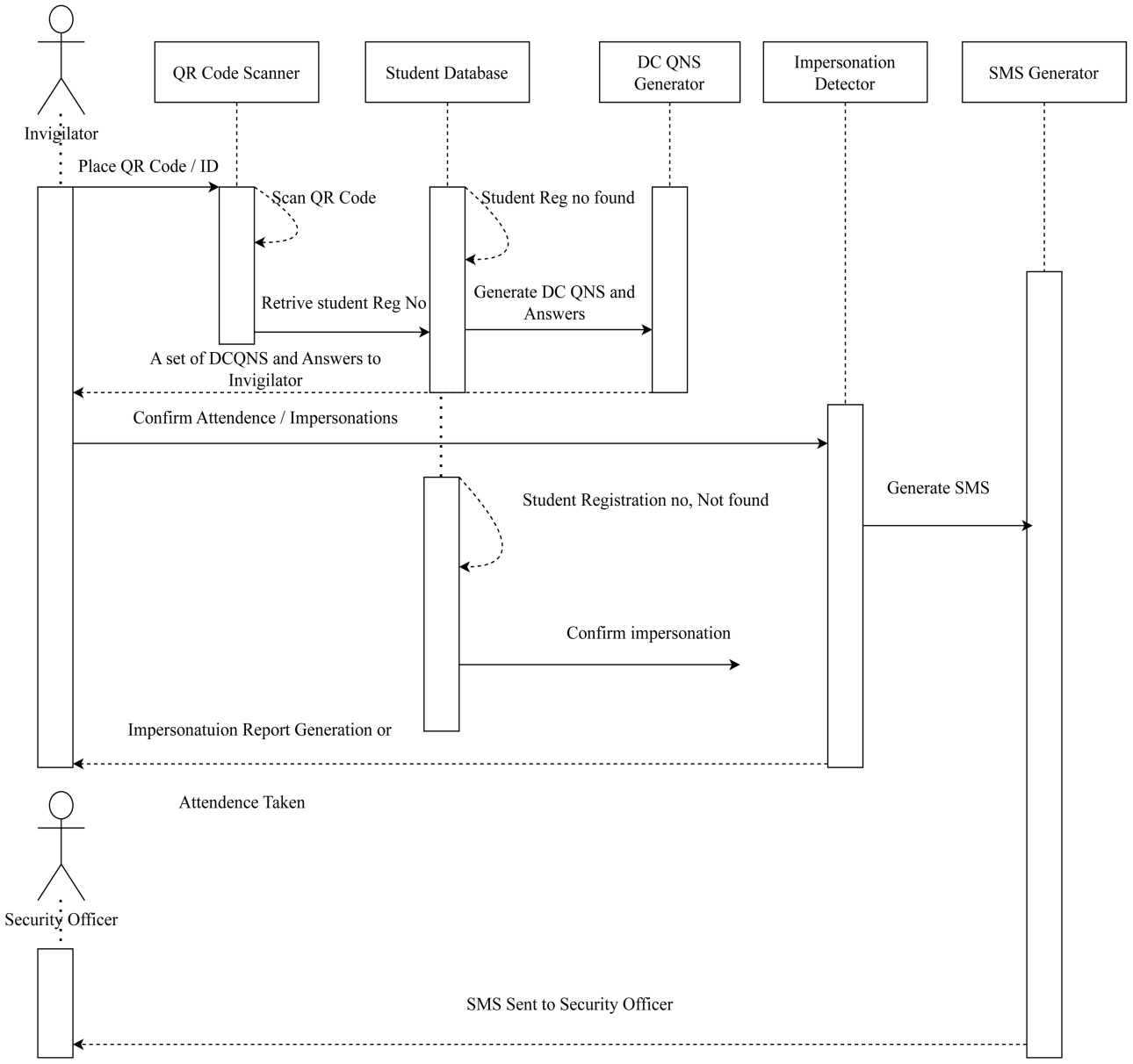

Figure 7. A Sequence diagram describing a scenario for student exam eligibility verification.

syndicated for further attention. Every confirmed impersonation is reported to the examination officer who is responsible for producing and submitting impersonation report to the deputy rector responsible for academic matters.

4.6.7. Taking Attendance

For every successful response an attendance is recorded along with student information (**Figure 3**).

4.6.8. Notifying Security Officer

The system sends message through a short message service which is integrated with the proposed system to a security officer dedicated to take care of security matters during examinations.

4.7. Implementation and Deployment of the Proposed Impersonation Detection System

The proposed system is made up of two subsystems, the mobile application and the web system. These two sub-systems communicate via respective application interfaces (APIs).

The Mobile Application was developed within 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 with 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 with 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 making it cost-effective for businesses and developers.

4.7.1. Implementation of the Mobile Application Client Side

The mobile 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, such features include: Single Codebase; Multiple Platforms; it saves time and effort compared to developing separate codebases for each platform; Fast Development; Flutter applications are compiled directly to native machine code, resulting in high performance and faster startup times; It utilizes Skia, a powerful graphics engine, to render UI components, ensuring smooth performance across different devices; offers plugins and platform channels that enable developers to access native platform features and APIs seamlessly; also it has Growing Community and Ecosystem; Open Source and Free and it is backed by Google, which provides ongoing support, updates, and improvements to the framework. Also flutter supports Dart Programming Language that provide features like ahead-of-time (AOT) compilation and just-in-time (JIT) compilation for efficient application development, 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 are written in Laravel code base and consumed to the application with secured baretokens on passing the data from server to the application to ensure that users using the data are authenticated users only (ie. Integration with RESTful APIs).

4.7.2. Implementation of the Web Server Side

The Web side was implemented with the 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 makes it easier to manage and maintain web applications, especially as they grow in complexity (Robust MVC Architecture); also Laravel has expressive syntax which provides an expressive and elegant syntax that simplifies common tasks such as routing, authentication, caching, and database operations. This allowed developers 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 applications quickly and efficiently. Moreover; the 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 to help developers protect their 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 make it easy to implement secure user authentication and access control; 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 supported by PhPMyadmin database tool to create, manipulate and manage the Database objects and assist the migrations from Laravel commands; again, 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 code mixed with PHP logic, 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 IMDIs application by integrating with services such as SMS gateways and cloud storage.

Overall, Laravel provided developer with a robust and feature-rich framework for building the IMDIs web server-side.

4.7.3. 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) algorithm is deployed in a mobile phone. These personalized questions are based on the student's profile stored in a MYSQL

database management system and the generated questions are designed to be answered correctly only by the legitimate student, enhancing security.

The web part of the system built with the Laravel Framework is deployed in SQL server or can be deployed in any relational database management system, the system manages the backend operations, including the generation of dynamic questions and communication with the database, which was implemented using MySQL. When a student arrives at the examination venue, the invigilator scans the QR code on the student's ID using the smart phone which is installed with student identity verification application. The application then generates and displays a set of dynamic questions on the smart phone screen (**Figure 2**).

Student must answer these questions correctly to be verified as a correct entity. This process typically takes around two (2) to four (4) 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 in the context of traditional-in-class examinations.

4.7.4. Summary

The integration of web and mobile application system which is developed with Laravel and Flutter frameworks 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. See **Figure 8** below describing the invigilator' application interface when he(s) is longed into the IMDIs application.

4.8. Evaluating the Proposed Improved Impersonations Detection System

4.8.1. Students Registration

In order to test functionalities of the proposed system, fifty (50) students from MNMA were enrolled into the system and registered for various examinations, these examinations include semester examinations, supplementary examinations, special examinations, and tests. Similar students were asked to exchange their profile information and try to perform abuse case scenarios. These students were given seven (7) days and were promised a lump sum of $50 to encourage them perform the security abuse case scenarios. Results from students' responses on abuse case scenarios are presented in section 4.8.2 to 4.8.5.

4.8.2. Usability Assessment and Efficiency of the Proposed Impersonation Detection System

The IMDIs system was able to generate 200 dynamic challenging questions based

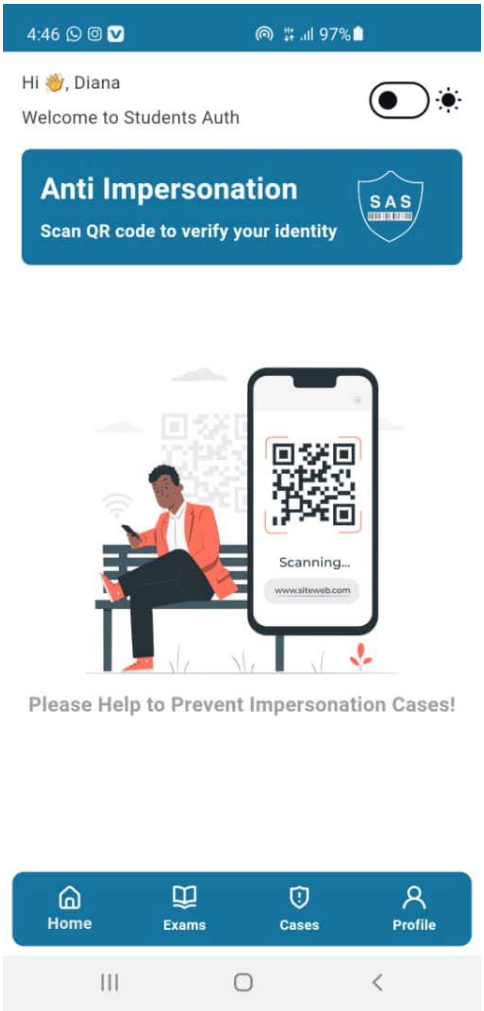

Figure 8. Application home page for verifying student's identity.

on different categories of student information along with their correct responses to verify the identity of 50 enrolled students. However, when impersonators came they failed to supply correct responses hence detected by the system as impersonators. But 50 valid students were able to respond to question generated by system therefore, they were correctly identified by the system. It was recommended that a system should generate 4 questions to avoid correct answers by chance (guessing attack). This indicates high system usability and efficiency.

4.8.3. Performing a Response Time Acceptance Testing

The IMDIs system takes 2 second to generate 4 different dynamic challenging questions and answers. This indicates that 200 students can be authenticated within 33 minutes per one system user (invigilator). This time can be reduced as the number of system operators increases.

4.8.4. Performing Some Analysis to Test the System's Reliability and Accuracy

To achieve the reliability and accuracy test, a false rejection (FR) and false

acceptance (FA) parameters were used [7].

To test for the false rejection, 50 students were registered and identified two times to check if the false rejection could occur (Table 1 shows the results). Results show that there were no false rejection in the proposed impersonation detection system as per 50 test dataset.

Table 1. Result from false rejection rate test carried out in the IMDIs system.

Total Sample	FR	FRR (%)
50	-	-

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

Again, results show that one student could be incorrectly accepted by the system hence there was one (1) false acceptance in the proposed impersonation detection system (see Table 2). The false acceptance rate could be reduced by either adding number of questions or complicating student profile.

Table 2. Result from falser acceptance test carried out in the IMDI system.

Total Sample	FA	FAR (%)
50	1	0.02

4.8.5. System Convenience

False Rejection Rate (FRR) scenarios were used to assess the convenience of the proposed impersonation detection system. Results show that the proposed impersonation detection system is convenient to the user with 1 (100%) convenience which is mathematically represented as follows [12].

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

Using Table 1, then

$$\text{Convenience} = 1 - 0 = 1\ (100\%)$$

4.8.6. Ensuring System Stability and Performance under Large-Scale Use

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 used 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 application 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 optimizing the codebase for both the mobile application and the backend system and ensure efficient use of resources and minimize latency in processing requests.

Other considerations include:

Regular Maintenance and Updates: Keeping the system updated with the latest security patches and performance improvements by regularly performing maintenance to ensure the system remains stable and secure.

Generally, 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.

4.8.7. Handling Misidentification of QR codes in the Proposed IMDIs System

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 allows 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 such as poor lighting and reflective surfaces.

Backup Identification Methods: A backup method 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.

Therefore, by incorporating these measures, the system can effectively handle misidentifications of QR codes, ensuring a smooth and reliable verification process.

4.8.8. System Security

Since the mathematical calculations presents that 0.02 FAR occurred during system testing, then it imperative to state that the mechanism (system) is 98% protected and perfect (see the mathematical derivation below).

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

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

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

5. Conclusion and Recommendations

5.1. Conclusion

The improved mechanism for detecting impersonations in traditional in-class exams integrates dynamic challenging questions and QR code technology to create a hybrid system for Tanzania's public higher learning institutions. By leveraging the compact, fast-scanning nature of QR codes and a dynamic question generation algorithm, the system enhances security by providing personalized, unpredictable questions unique to each student. Assessments showed impersonators could only answer 25% to 50% of questions correctly, proving its effectiveness. The system verifies student eligibility within two seconds, with a 2% false acceptance rate, 0% false rejection rate, and 98% security, ensuring both reliability and user-friendliness.

5.2. Recommendations

Future efforts can focus on exploring modalities for interacting with the proposed dynamic challenging questions student verification system and advancing the development of a comprehensive mechanism on a larger scale. This will ultimately result in the construction of a comprehensive impersonations detection mechanism that integrates with existing institutional systems, such as students' academic records systems, examination records systems, and payment systems. This integration has the potential to be applied in the large scale student examinations verification model.

Acknowledgements

I would like to express my deepest gratitude to my supervisors, Dr. Rogers Philip Bhalalusesa and Dr. Selemani Ismail for their unwavering guidance, invaluable feedback, and continuous support throughout the duration of this research. Their expertise, encouragement, and patience have been instrumental in shaping this work. I am also grateful to the faculty members of the Department of Mathematics, Information and Communication Technology of the OUT for their insightful comments and suggestions, which have enhanced the quality of this work. 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 understanding, encouragement, and unwavering belief in my abilities. Their moral support has been a source of strength and motivation during challenging times. Additionally, I would like to acknowledge the assistance provided by Alphaxsad Kakulu, Ramadhan Ramadhan, Dr. Sixbert Msambichaka, Mis. Diana Mdope and Mr. Denis Malele for their contributions to data collection, data analysis and system development.

Finally, I am indebted to the participants of this study for their willingness to share their experiences and insights, without which this research would not have been possible.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Muhammad, B.A., Zahra'u, M.N. and Lawal, M.J. (2018) Examination Eligibility Verification and Attendance System Using Quick Response Code. *I-Manager's Journal on Digital Signal Processing*, **6**, 1-9.

[2] Akaranga, S.I. and Ongong, J.J. (2013) The Phenomenon of Examination Malpractice: An Example of Nairobi and Kenyatta Universities. *Journal of Education and Practice*, **4**, 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=

[3] Akinola, O.A., Abayomi-Alli, A. and Adeniyi, R.A. (2015) Development of a Microcontroller Based Fingerprint Examination Access Control System. *African Journal of Computing & ICT*, **8**, 145-152. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Development+of+a+Microcontroller+Based+Fingerprint+Examination+Access+Control+System&btnG

[4] Kilani, M.A. and Kobziev, V. (2016) An Overview of Research Methodology in Information System (IS). *Open Access Library Journal*, **3**, e3126.

[5] Aramide, K.A., Ladipo, S.O. and Adebayo, I. (2015) Demographic Variables and ICT Access as Predictors of Information Communication Technologies' Usage among Science Teachers in Federal Unity Schools in Nigeria. *Library Philosophy and Practice* (*e-Journal*), 1217. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=3208&context=libphilprac

[6] 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 Research in Science*, *Engineering and Technology*, **3**, 1-16. 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=

[7] Baijnath, N. and Singh, D. (2019) Examination Cheating: Risks to the Quality and Integrity of Higher Education. *South African Journal of Science*, **115**, Article No.

6281. https://doi.org/10.17159/sajs.2019/6281

[8] Diedenhofen, B. and Musch, J. (2016) Pagefocus: Using Paradata to Detect and Prevent Cheating on Online Achievement Tests. *Behavior Research Methods*, **49**, 1444-1459. https://doi.org/10.3758/s13428-016-0800-7

[9] Elaskari, S., Imran, M., Elaskri, A. and Almasoudi, A. (2021) Using Barcode to Track Student Attendance and Assets in Higher Education Institutions. *Procedia Computer Science*, **184**, 226-233. https://doi.org/10.1016/j.procs.2021.04.005

[10] 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*, **3**, 1-16.

[11] Kothari, C. and Garg, G. (2014) Research Methodology Methods and Techniques. 3rd Edition, New Age International (P) Ltd.

[12] Lourde, R.M. and Khosla, D. (2010) Fingerprint Identification in Biometric Security Systems. *International Journal of Computer and Electrical Engineering*, **2**, 852-855. https://doi.org/10.7763/ijcee.2010.v2.239

[13] Madara, D. and Namango, S. (2016) Faculty Perceptions on Cheating in Examinations in Undergraduate Engineering. *Journal of Education and Practice*, **7**, 30. http://www.iiste.org/

[14] Oladele, M.O., Adepoju, T.M., Olatoke, O.A. and Ojo, O.A. (2020) Offline Yorùbá Handwritten Word Recognition Using Geometric Feature Extraction and Support Vector Machine Classifier. *Malaysian Journal of Computing*, **5**, 504-514. https://doi.org/10.24191/mjoc.v5i2.8947

[15] Rufai, M.M., Adigun, J.O. and 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*, **2**, 120-124.

[16] Onuka, A. and Durowoju, E. (2011) Curtailing Examination Fraud for Improved Quality Assurance in the African Examination System. *Journal of Educational Assessment in Africa*, **6**, 27-38. http://ir.library.ui.edu.ng/handle/123456789/2514

[17] Patton, M. (2015) Qualitative Research and Evaluation Methods. 4th Edition, Sage Publications.

[18] Saheed, Y.K., Hambali, M.A., Adedeji, A.A. and Adeniji, I.A. (2016) Attendance Management System Using Barcode Identification on Students' Identity Cards. *The Pacific Journal of Science and Technology*, **17**, 224-230. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Attendance+Management+System+Using+Barcode+Identification+on+Students%E2%80%99+Identity+Cards&btnG=

[19] Tanzania Commission for Universities (2021/2022) Undergraduate Admission Guidebook. https://www.tcu.go.tz

[20] TCU (2021) VitalStats. https://www.tcu.go.tz

[21] The Mwalimu Nyerere Memorial Academy Prospectus (2023/2024) Dar es Salaam.

[22] Tomas de Aquino, Y.C. (2022) Teacher Training vs. Trainer Training in Education. *International Journal of Research and Innovation in Social Science* (*IJRISS*), **6**, 709-715. https://ideas.repec.org/a/bcp/journl/v6y2022i8p709-715.html

[23] Uchenna, M.M. and 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, **2**, 52-62. https://www.noveltyjournals.com

[24] Ullah, A., Xiao, H. and Barker, T. (2018) A Dynamic Profile Questions Approach to Mitigate Impersonation in Online Examinations. *Journal of Grid Computing*, **17**, 209-223. https://doi.org/10.1007/s10723-018-9442-6

[25] Yamane, T. (1967) Statistics: An Introductory Analysis. 2nd Edition, Harper and Row.

[26] Abu-Shanab, E.A. (2011) Education Level as a Technology Adoption Moderator. 2011 3*rd International Conference on Computer Research and Development*, Shanghai, 11-13 March 2011, 324-328. https://doi.org/10.1109/iccrd.2011.5764029