CAVENDISH UNIVERSITY ZAMBIA

BSC COMP

Research/Project Proposal

FALCUTY NAME: BUSINESS INFORMATION TECHNOLOGY

RESEARH/ PROJECT TITLE: DOCKET VERIFICATION SYSTEM.

STUDENT NAME: DENISE SETI AND REWARDSON BUKURU

STUDENT NUMBER: 104-744 AND 104-775

YEAR: 2025

CHAPTER ONE: INTRODUCTION

1.0 Introduction

Universities worldwide rely on exam dockets as an essential tool to control and monitor student eligibility during examinations. Traditionally, such dockets were issued physically after finance clearance, but many institutions have now adopted online systems to reduce long queues and improve efficiency. However, the shift to digital portals has also introduced new challenges, one of the most pressing being the forgery of exam dockets.

Globally, universities have responded to this challenge by embedding unique identifiers, QR codes, or digital signatures into examination-related documents to ensure authenticity. In Zambia, Cavendish University has moved from manual docket issuance by Finance and Retentions offices to allowing students to directly download them from the student portal. While this change reduced congestion, it has created opportunities for students to forge or manipulate dockets, thereby undermining credibility and examination security.

This study therefore proposes the design and implementation of a **docket verification system** integrated into the student portal. The system will generate unique machine-readable barcodes or QR codes for each docket, linked to a central database. Verification will be done through edge computing devices (such as laptops or mobile phones) at exam venues, ensuring instant authentication even without continuous internet connectivity.

1.1 Background

Exam dockets are a critical requirement that proves a student's financial clearance and eligibility to sit for examinations. Previously, Cavendish University required students to physically collect dockets after verification by Finance and Retentions departments. However, due to long queues and administrative bottlenecks, this process was shifted to the student portal, where students who have cleared their payments can directly download their dockets.

While this system improved accessibility, it introduced a major loophole: the possibility of forging or tampering with downloaded documents. Students with insufficient clearance have in some cases edited or duplicated docket files. The absence of strong verification measures has made this malpractice difficult to detect during examinations.

To bridge this gap, modern digital solutions such as QR codes, blockchain verification, and digital signatures have been employed in other institutions. Adopting a similar but simplified approach suitable for Cavendish University will reduce malpractice and improve the credibility of the examination process.

1.2 Motivation of the Study

The main motivation behind this project is to address the growing problem of forged exam dockets at Cavendish University. By creating a system that can quickly and reliably verify

docket authenticity, the project will not only safeguard academic integrity but also build trust in digital processes introduced by the University. Furthermore, the project offers students the opportunity to apply software engineering principles to a real-life institutional challenge.

1.3 Significance of the Study

The proposed system is significant in several ways:

- It will help Cavendish University curb forgery of exam dockets, protecting the integrity of examinations.
- It will provide a scalable and efficient verification mechanism that reduces reliance on manual checks.
- It will serve as a model for other universities in Zambia facing similar challenges.
- For students, the project demonstrates how real-world problems can be addressed through innovative use of software engineering and edge computing concepts.

1.4 Scope of the Study

The project will focus on the design and implementation of a prototype docket verification system. It will simulate Cavendish University's student portal using a cloned environment with a student database containing sample records. The system will generate exam dockets embedded with barcodes/QR codes and implement a verification application that can operate on edge devices. The study will not cover integration with actual financial systems or full deployment within the University, but will instead present a functional prototype.

1.5 Problem Statement

While Cavendish University shifted from manual to portal-based exam docket issuance to improve efficiency, this change has led to increased forgery of dockets. Students who have not cleared their financial obligations can manipulate or fake downloaded documents. The lack of an automated verification system makes it difficult for invigilators to distinguish genuine from forged dockets during examinations, thus compromising examination integrity.

1.6 Objectives

1.6.1 General Objective

To design and implement an exam docket verification system using barcodes and edge computing to prevent docket forgery at Cavendish University.

1.6.2 Specific Objectives

1. To analyze the current exam docket issuance process at Cavendish University and identify loopholes leading to forgery.

2. To design a prototype database and portal capable of issuing unique dockets linked to student clearance records.
3. To implement a barcode/QR code system that ensures each docket is uniquely identifiable.
4. To develop a verification application that can authenticate dockets on edge devices without full reliance on internet connectivity.
5. To test the system with simulated student records to demonstrate scalability and robustness.

1.7 Research Questions

1. What weaknesses in the current exam docket issuance system contribute to forgery?
2. How can barcodes or QR codes be integrated into exam dockets to ensure uniqueness and prevent duplication?
3. What database structure is required to support secure and scalable docket issuance?
4. How can edge computing be used to verify dockets efficiently in offline or semiconnected environments?
5. How effective is the proposed system in detecting forged dockets during testing?

1.8 Conceptual/Theoretical Framework

This study is based on principles of **information security** and **edge computing**. The information security framework ensures authenticity, integrity, and non-repudiation of exam dockets through unique identifiers and digital signatures. Edge computing theory supports local verification on decentralized devices to reduce dependence on a central server, ensuring fast response times during examinations.

1.9 Definition of Terms

- **Exam Docket:** An official document issued to students confirming eligibility to sit for examinations.
- **Forgery:** The act of producing a false version of a document with intent to deceive.
- **Edge Computing:** Processing data locally on devices rather than relying exclusively on a central server.
- **QR Code/Barcode:** Machine-readable symbols encoding unique data linked to a database.

1.10 Organization of the Report

The report is organized into three chapters. Chapter One introduces the problem, objectives, and scope of the study. Chapter Two reviews related literature and identifies research gaps. Chapter Three outlines the research design, methodology, and system development approach.

CHAPTER TWO: LITERATURE REVIEW

2.0 Overview

A literature review provides an analysis of existing research related to the problem under investigation. It highlights what has been done globally and locally, identifies gaps, and positions the proposed study as a response to those gaps. For this study, the focus is on digital verification systems, the use of barcodes and QR codes in document security, and the application of edge computing in education.

2.1 Literature Review

Global Perspective

Globally, universities and examination bodies have faced challenges related to document forgery. Academic documents such as transcripts, certificates, and exam passes are often targeted for manipulation (Chauhan & Jain, 2020). To counter this, institutions have increasingly adopted technologies like QR codes, digital watermarks, and blockchain verification (Mohanty et al., 2019). For example, in India, the University Grants Commission introduced the National Academic Depository (NAD), where verified academic records are stored digitally, reducing the risk of forgery (UGC, 2018).

In Europe and the United States, QR codes are widely embedded in official student documents to enable quick verification using mobile applications (Petrisor, 2019). Similarly, blockchain technology has been proposed to create tamper-proof educational records, although the high costs and technical complexity often limit its adoption in developing countries (Tapscott & Tapscott, 2017).

Regional and Local Perspective

In Africa, many universities have begun digitizing administrative services to reduce congestion and improve efficiency (Ngugi, 2021). However, the transition has often exposed weaknesses in document security. For instance, some Zambian universities issue exam dockets through online portals without robust verification mechanisms, creating opportunities for forgery. Research by Musonda (2020) highlights that while digital systems improve accessibility, their security features are often overlooked, leading to the circulation of fake academic documents.

Use of Barcodes and QR Codes

Barcodes and QR codes are low-cost, reliable technologies for verifying the authenticity of documents (Liu & Dai, 2019). A QR code can store encrypted information such as student ID, exam ID, and clearance status, which can be validated against a database. This method has been

used successfully in examination passes in countries like China and South Africa (Zhang, 2018). Unlike simple PDFs or printed slips, barcoded dockets are harder to forge because the code must match database records during scanning.

Edge Computing in Verification Systems

Edge computing is increasingly being applied in education to reduce latency and improve offline access (Shi et al., 2016). By enabling verification at local devices rather than a central server, institutions can avoid bottlenecks and network failures. For instance, in Kenya, mobile-based edge solutions were tested for exam verification to allow offline validation in rural areas (Omondi, 2021). Applying this approach to Cavendish University means that invigilators can instantly check docket authenticity at exam halls, even without stable internet connectivity.

2.2 Related Works

Several studies have proposed frameworks for preventing academic document forgery. Mohanty et al. (2019) designed a QR-based system for examination passes, while Musonda (2020) investigated security challenges in Zambian universities' e-learning platforms. Petrisor (2019) studied QR-enabled transcripts in Europe, while Omondi (2021) demonstrated mobile-based offline verification in East Africa.

However, few studies have combined **barcodes/QR codes with edge computing in the Zambian higher education context**. Most local universities focus on online portals but lack offline verification mechanisms, leaving room for forgery when documents are printed or shared outside the system.

2.3 Gaps in the Literature

From the reviewed literature, it is clear that:

1. Many global solutions rely on advanced systems such as blockchain, which may be costly for developing countries.
2. Local Zambian universities have digitized docket issuance but **lack strong verification methods** to prevent forgery.
3. Few studies have considered the use of **edge computing** to enable instant verification in exam halls, especially in environments with unreliable internet.

This study therefore seeks to fill these gaps by proposing a **cost-effective, barcode-based docket verification system integrated with edge computing**, specifically tailored for Cavendish University.

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

3.0 Overview

This chapter explains in detail how the proposed exam docket verification system will be designed, developed, and tested. The methodology provides a roadmap for the project, beginning with identifying the problem, gathering requirements, designing the system, and finally developing and testing the solution. Since this is a practical software project, the methodology combines research with software engineering principles.

3.1 Research Design

The project follows a **Design Science Research Methodology (DSRM)**. This means the research is not just about studying the problem of docket forgery but about **building a working solution** that can solve it.

The design science process includes the following stages:

1. **Problem Identification** – Clearly define the challenge of forged exam dockets at Cavendish University.
2. **Objectives of the Solution** – State what the system should achieve, such as uniqueness of dockets and quick verification.
3. **Design and Development** – Build the actual prototype system (database, portal, barcode generation, and verification).
4. **Demonstration** – Show how the system works by using sample student data and test cases.
5. **Evaluation** – Test if the system actually prevents forgery and is easy to use.
6. **Communication** – Document and present findings to show the value of the project.

This approach ensures the project is **practical, problem-oriented, and results in a tangible solution.**

3.2 Baseline Study

3.2.1 Data Collection

Since we do not have direct access to Cavendish University's real student finance data, we will simulate it. A **dummy student database** will be created with at least 5,000–10,000 fake records to demonstrate scalability. Each record will contain:

- Student ID
- Student Name
- Program of study and year
- Finance clearance status (cleared/not cleared)
- Docket ID
- Issue date

This setup allows us to test how the system works as if it were running in the real university environment.

We will also review existing docket samples and the current student portal to understand how data currently flows from finance clearance → portal → student download.

3.2.2 Research Approach

The project will use a **quantitative approach**. This means after the system is built, we will measure:

- **Speed** (how fast the verification happens when scanning a docket).
- **Accuracy** (whether the system can correctly identify fake vs. genuine dockets).
- **Scalability** (how well the system performs when many students are processed at once).

3.2.3 Development of the Application

The project will follow **incremental prototyping**, meaning we will build the system in small parts, test each part, and then improve it.

Steps include:

1. **Database Creation** – Build a MySQL database that stores student and finance records.
2. **Portal Simulation** – Clone a simplified version of the student portal where students can log in and download their dockets.
3. **Docket Generation** – Once cleared, the system generates an exam docket with a **unique barcode/QR code**. The code contains encrypted data such as student ID, docket ID, and clearance status.
4. **Verification Module** – Develop a verification tool (either a web app or mobile app) that can scan the barcode/QR code and instantly check if it matches the database.

5. **Edge Computing Integration** – The verification module will have a **local copy (cache)** of the student data. This means even if the internet goes down in the exam hall, invigilators can still verify dockets offline. Later, the system can sync with the central database when the internet is back.
6. **Testing** – Simulate students entering an exam hall and verify whether the system can quickly detect forged dockets.

3.3 System Design

3.3.1 Context Diagram

- **Student:** Logs in to the portal → downloads docket with barcode.
- **Finance Admin:** Updates clearance records in the finance database.
- **System:** Issues dockets only if clearance is confirmed.
- **Verifier (Exam Invigilator):** Scans barcode on the docket → system checks if valid → displays result (VALID or INVALID).

3.3.2 System Software Architecture

The system will be built in **three layers**:

1. **Presentation Layer (Frontend):** Student portal and verifier interface.
2. **Application Layer (Backend):** Business logic that generates dockets and processes verification.
3. **Database Layer:** Stores all student, finance, and docket information. A **local cache database** will also be kept for offline verification.

3.3.3 Modular Design

The system will have the following main modules:

1. **Student Module:** Allows login and docket download.
2. **Finance Module:** Records student clearance.
3. **Docket Module:** Generates dockets with barcodes.
4. **Verification Module:** Scans and validates barcodes.
5. **Audit Logs:** Keeps records of every verification for accountability.

3.3.4 Class Diagram (Simplified)

- **Student** (student_id, name, program, year)
- **Finance** (student_id, amount_paid, clearance_status)
- **Docket** (docket_id, student_id, barcode, issue_date, status)
- **Verifier** (verifier_id, scan_time, docket_id, result)

3.3.5 Data Model Design

Four key tables will be implemented:

1. **Students** – student_id, name, program, year.
2. **Finance** – student_id, amount_paid, clearance_status.
3. **Dockets** – docket_id, student_id, barcode, issue_date, status. 4. **VerificationLogs** – verifier_id, docket_id, scan_time, result.

3.4 Hardware and Software Requirements

Hardware Requirements:

- Laptop with at least 4GB RAM and 500GB HDD.
- Smartphone camera or laptop webcam (for scanning barcodes).
- No expensive servers needed, since edge computing allows local devices to verify.

Software Requirements:

- **Backend/Database:** MySQL with XAMPP.
- **Frontend:** HTML, CSS, Bootstrap (for portal simulation).
- **Programming Language:** PHP or Python Flask.
- **Libraries:** php-barcode, python-barcode, pyzbar (for QR/barcode generation and scanning).
- **IDE:** Visual Studio Code.

3.5 Time Frame

The project will take **5 weeks**, broken down as follows:

- **Week 1:** System design, database setup, and literature review finalization.
- **Week 2:** Build student portal simulation and finance module.
- **Week 3:** Implement docket generation with barcodes.
- **Week 4:** Build verification module + offline (edge) functionality.
- **Week 5:** Testing, debugging, documentation, and proposal finalization.

3.6 Budget

The budget is minimal because the project uses **open-source software** and **existing hardware** (student laptops and phones). No additional financial costs are expected apart from internet bundles for testing and electricity for running devices.

REFERENCES

- Chauhan, A., & Jain, R. (2020). *Document Security in Higher Education: Challenges and Solutions*. International Journal of Computer Applications.
- Liu, Y., & Dai, H. (2019). *QR Codes in Document Authentication*. Journal of Information Security.
- Mohanty, P., Panda, S., & Rath, A. (2019). *Preventing Examination Malpractice Using QR Technology*. Asian Journal of Computer Science.
- Musonda, C. (2020). *Digital Security Gaps in Zambian Universities*. Lusaka Journal of ICT.
- Ngugi, P. (2021). *Digitization of Higher Education Administration in Africa*. African ICT Review.
- Omondi, J. (2021). *Mobile-Based Verification Systems in Education*. East African ICT Journal.
- Petrisor, A. (2019). *QR-enabled Academic Documents in Europe*. Journal of Educational Technology.
- Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). *Edge Computing: Vision and Challenges*. IEEE Internet of Things Journal.
- Tapscott, D., & Tapscott, A. (2017). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin.
- UGC. (2018). *National Academic Depository*. University Grants Commission, India.
- Zhang, L. (2018). *QR Codes for Exam Admission Security in China*. Journal of eGovernance.