ABOUT THE INNOVATOR

NAME: BORNFACE SONYE

REG NO: COM/B/01-00106/2018

PHONE NUMBER: 0798073204

EMAIL: bornfacesonye@gmail.com

PROJECT TITLE

GPS: Proposed Integrated Gate Pass System for Masinde Muliro University of Science and Technology

CHAPTER ONE: INTRODUCTION

1.1 Introduction to GPS

1.2 Statement of the problem

1.3 Main aim of the project

1.4 Specific objectives of the project

1.5 Research questions

1.6 Scope of the project

1.7 Limitations of the study

1.8 Benefits and beneficiaries of the study

1.9 Rational of implementing the project

1.1 Introduction to GPS

GPS is a proposed integrated digital solution designed to streamline campus access, improve security, and reduce inefficiencies.

1.2 Statement of the problem

- Manual gate pass checks at MMUST lead to long queues, delays, and security risks.
- Lack of proper tracking allows unauthorized individuals to enter, increasing theft and other security threats.
- The current process does not provide data on the number of individuals on campus or their movement, limiting effective security planning and management.

1.3 Main aim of the project

To develop a digital Gate Pass System that enhances campus security, streamlines access processes, and provides real-time data on campus traffic, ensuring only authorized personnel can enter university premises.

1.4 Specific objectives of the project

i. To design a user-friendly system for students, staff, and guests to register and access campus digitally.

ii. To develop a security module for real-time monitoring and access control.

iii. To Integrate item tracking (e.g., laptops, vehicles) to prevent unauthorized removal from the premises.

1.5 Research questions

i. How can digital solutions improve campus security and reduce unauthorized access?

ii. What system design best addresses the current inefficiencies in gate pass management at MMUST?

iii. How can real-time data improve security and operational planning within the university?

iv. How can the system balance security with ease of access for students, staff, and guests?

1.6 Scope of the project

- **Geographic Scope:** Focus on the main campus of Masinde Muliro University of Science and Technology.
- **Functional Scope:** Includes student, staff, guest registration, security monitoring, and item tracking.
- **Technological Scope:** Involves web and USSD interfaces, integrated with university ERP for data access and management.

1.7 Limitations of the study

- **Technology Accessibility:** Some users may lack access to smartphones or internet connectivity, requiring USSD support.
- **User Adoption:** Resistance to adopting new digital processes from both security staff and users may delay full implementation.
- **Budget Constraints:** Limited funding may restrict advanced features like AI-based monitoring and analysis.

1.8 Benefits and beneficiaries of the study

- **University Security Department:** Improved access control and better data for security management.
- **Students, Staff, and Guests:** More efficient campus access, reduced delays, and enhanced security for personal items.
- **University Administration:** Ability to track campus traffic, plan for resource allocation, and ensure secure campus operations.
- **Developers:** Students involved in system development gain practical experience and skills.

1.9 Project Justification

- **Enhanced Security:** The GPS will provide a modern solution to safeguard university premises, reducing unauthorized access and theft.
- **Operational Efficiency:** Automation of gate pass processes will eliminate queues and delays, improving campus operations.
- **Data-Driven Decisions:** The system will offer valuable data for managing security, resource allocation, and monitoring campus traffic.
- **Scalable Solution:** The GPS can be extended to other universities, potentially generating revenue for MMUST through licensing agreements.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

2.2 Overview of Current University Access Systems in Kenya

2.3 Existing Technologies for Campus Security in Kenyan Universities

2.4 Critique of Existing Solutions in Kenyan Universities

2.5 Gaps in Existing Research

2.1 Introduction

This chapter provides a review of current security systems used in Kenyan universities, focusing on access control and campus security.

It critiques existing manual and digital systems for managing campus entry and exit, identifies their shortcomings, and presents the need for a more effective, data-driven solution.

The review emphasizes the necessity of improving security processes in line with technological advancements and the growing need for robust access management in academic institutions.

2.2 Overview of Current University Access Systems in Kenya

- **Manual Systems:** Many Kenyan universities, including Masinde Muliro University of Science and Technology (MMUST), University of Nairobi (UoN), and Kenyatta University (KU), rely on manual systems for managing campus entry. These involve physical gate passes, ID cards, and registration forms, which are slow, prone to errors, and often cause long queues.
- **Digital Systems:** Some institutions, such as Strathmore University and USIU-Africa, have started implementing digital solutions like RFID-based access or smart card systems to streamline entry, but these solutions still have limitations in handling high traffic and item security.

2.3 Existing Technologies for Campus Security in Kenyan Universities

- **RFID-Based Access Systems:** Institutions like Strathmore University use RFID tags for student and staff entry, allowing for faster access control. However, the system does not extend to guest management, and there is no provision for tracking personal items like laptops or vehicles.
- **Biometric Systems:** Universities such as Kenyatta University and Jomo Kenyatta University of Agriculture and Technology (JKUAT) have explored biometric systems for exam registration and access control. While these systems provide better security, they often come with high costs, maintenance challenges, and limited scalability for managing campus-wide security.
- **Smart Card-Based Access:** Some universities, such as United States International University (USIU-A), have adopted smart card-based systems, which improve identity verification but still do not effectively address delays or track valuable personal items.

2.4 Critique of Existing Solutions in Kenyan Universities

- **Manual Gate Passes:** Systems like those in MMUST and Egerton University rely on students and staff filling out physical gate passes when entering or exiting with personal items like laptops. This process is time-consuming, prone to delays, and lacks adequate tracking, leading to security loopholes.
- **Limited Item Security:** Few universities have systems that track personal belongings, such as laptops, phones, or vehicles. This leaves room for theft, as stolen items are often difficult to trace once inside the premises.
- **Lack of Real-Time Monitoring:** Current systems fail to provide real-time data on campus traffic, limiting the ability of security personnel to respond swiftly to incidents or prevent unauthorized access. This challenge is evident in larger institutions like UoN, where multiple campuses make it difficult to monitor and control movements.

2.5 Gaps in Existing Research

- **Guest Management:** Most Kenyan universities lack a streamlined system for managing guest access. Visitors typically sign in manually, with no record of frequent visitors or their activities, as seen in institutions like KU and MMUST.
- **Multi-Channel Access:** While some digital solutions exist, most universities do not offer options like USSD for those without access to smartphones or the internet. This digital divide leaves a significant portion of users dependent on manual systems.
- **Lack of Item Tracking:** Current systems do not provide robust mechanisms for tracking high-value personal items like laptops or vehicles, which are often stolen on campus. This is a notable issue at universities with larger student populations like Moi University.
- **Underutilization of Data:** Kenyan universities are not leveraging real-time security data for predictive analysis, which could enhance resource allocation and security planning. Systems could be more intelligent by using data to predict peak access times and prevent congestion at entry points.

CHAPTER THREE: METHODOLOGY

3.1 Introduction

3.2 Target users of the product

3.3 Target population

3.4 Sample population and how it was arrived at

3.5 Methods of data collection

3.6 System requirements

3.7 Software development methodology

3.1 Introduction

This chapter outlines the research methodology employed to develop the Gate Pass System (GPS) for Masinde Muliro University of Science and Technology (MMUST).

It includes details about the target users, population, data collection methods, system requirements, and the software development methodology chosen for this project.

3.2 Target users of the product

The primary users of the Gate Pass System will include:

- **Students:** Regular users accessing university facilities and resources.
- **Staff:** Employees of MMUST who need to access different areas for work-related purposes.
- **Guests:** Visitors attending university events or meeting with staff and students.
- **Security Personnel:** Officers responsible for managing and monitoring campus access.

3.3 Target population

The target population for the study includes:

- **Students:** Approximately 10,000 enrolled at MMUST.
- **Staff:** About 1,500 academic and administrative personnel.
- **Guests:** Variable, depending on events and activities, averaging 1000 visitors per month.

This population is chosen to ensure comprehensive insights into user needs and system requirements across various user groups.

3.4 Sample population and how it was arrived at

A sample population of 400 individuals was determined, comprising:

Students: 300 (75% of the sample)

Staff: 80 (20% of the sample)

Guests: 20 (5% of the sample)

The sample was selected using stratified random sampling to ensure representation across different user categories, taking into account factors such as year of study, faculty, and staff roles.

This method ensures a balanced view of user experiences and requirements, enhancing the validity of the study results.

3.5 Methods of data collection

Interviews:

Conducted with security personnel and a selection of students and staff to gather in-depth qualitative data about existing access challenges. Chosen for their ability to capture detailed insights and perspectives from users with varied experiences.

Observation:

Conducted at entry points of MMUST to assess the current access process, including time taken and the frequency of incidents (e.g., queues, unauthorized access). Chosen for its ability to provide real-time data on the effectiveness of existing systems and identify specific areas needing improvement.

3.6 System requirements

3.6.1 Hardware Requirements

3.6.2 Software Requirements

3.6.1 Hardware Requirements

- **Server:** A dedicated server with sufficient storage and processing power for hosting the GPS.
- **User Devices:** Personal computers and mobile devices (smartphones) for students, staff, and guests to access the system.
- **Networking Equipment:** Routers and access points to ensure stable internet connectivity across campus.

3.6.2 Software Requirements

3.6.2.1 Functional Requirements

3.6.2.2 Non Functional Requirements

3.6.2.1 Functional Requirements

REQ-1: The system shall allow students, staff, and administrators to register using data from the university's ERP system.

REQ-2: The system shall allow guests to register and create a temporary account for a single visit or maintain an account for frequent visits.

REQ-3: The system shall provide an option for users to update their personal information.

REQ-4: The system shall require users to log in using their university credentials (e.g., student/staff ID and password).

REQ-5: The system shall provide options for password recovery for users who forget their credentials.

3.6.2.1 Functional Requirements

REQ-6: The system shall allow users to select the type of access (Entrance or Exit).

REQ-7: The system shall allow users to specify the area they wish to access (e.g., specific gates or buildings).

REQ-8: The system shall allow users to schedule access in advance and cancel their schedules up to 30 minutes before the scheduled time.

REQ-9: The system shall allow users to input details of items they are carrying, including electronic devices and vehicles.

REQ-10: The system shall generate a unique serial number for each entry request, valid until midnight of the day of the visit.

3.6.2.1 Functional Requirements

REQ-11: The system shall send the unique serial number to the user via SMS or email upon successful registration of the entry.

REQ-12: Security officers shall verify the user's unique serial number and the details of the items they are carrying against the system records.

REQ-13: The system shall allow security officers to grant or deny access based on successful verification.

REQ-14: The system shall log all entry and exit attempts, including time stamps and verification results.

REQ-15: The system shall follow the same verification process upon exit to ensure all items are accounted for.

3.6.2.1 Functional Requirements

REQ-16: The system shall update the user's status to indicate they have left the premises.

REQ-17: The system shall generate reports on campus traffic, including the number of entries and exits, for analysis by the security department.

REQ-18: The system shall allow academic staff to access student movement data for monitoring attendance and activities.

3.6.2.2 Non Functional Requirements

NFR-1: The system should handle up to 10,000 concurrent users without performance degradation.

NFR-2: Response times for user actions (login, registration, access requests, etc.) should not exceed 2 seconds during normal operations.

NFR-3: The system should process access requests and generate unique serial numbers in less than 1 second during peak hours.

NFR-4: The system should be scalable to accommodate future expansion to all departments and campuses of MMUST.

NFR-5: The system architecture should allow for additional modules (e.g., USSD interface, examination verification system) without requiring major changes to the core infrastructure.

3.6.2.2 Non Functional Requirements

NFR-6: The system should handle a growing number of users and entries/exits, supporting at least a 50% increase in users over the next 5 years.

NFR-7: The system should enforce strong user authentication (e.g., university credentials) to prevent unauthorized access.

NFR-8: All sensitive data (e.g., passwords, unique serial numbers, personal information) should be encrypted both at rest and in transit using industry-standard encryption protocols (e.g., AES-256).

NFR-9: The system should implement role-based access control (RBAC) to ensure that only authorized personnel (e.g., security officers) have access to critical system functions.

NFR-10: Regular security audits and vulnerability assessments should be conducted to identify and mitigate potential security threats.

3.6.2.2 Non Functional Requirements

NFR-11: The user interface (UI) should be intuitive, with clear instructions and easy navigation, ensuring users with basic digital literacy can operate the system.

NFR-12: The system should be accessible to users with disabilities by adhering to web accessibility standards such as WCAG 2.1 Level AA.

NFR-13: The USSD interface should be simple and efficient, allowing users to complete access requests within 3-5 steps.

NFR-14: The system should maintain a minimum uptime of 99.9% annually, ensuring continuous availability for users.

NFR-15: The system should have built-in redundancy for critical components, ensuring it remains operational in case of hardware or software failures

3.7 Software development methodology

Chosen Methodology: Agile Development

Justification:

Flexibility: Agile allows for iterative development, enabling regular feedback from users and stakeholders, which is crucial for a user-centered system like the GPS.

Rapid Prototyping: Quick iterations and prototypes can be developed and tested within the university environment, facilitating adjustments based on user feedback.

Collaboration: Promotes active collaboration between developers, security personnel, and university management, ensuring the system meets the diverse needs of all user groups.

Continuous Improvement: Agile methodology supports ongoing improvements based on real-time user interactions and evolving requirements, essential for a security system that must adapt to various scenarios and threats.

APPENDICES

A. Development tools and technologies

B. Project Schedule

C. Project Budget

A. Development tools and technologies

Frontend Development: React.js with Material UI

Backend Development: ASP.NET Core

Database: SQL Server

Hosting: Microsoft Azure

Development Environment: Visual Studio

Version Control: Git and GitHub

USSD Integration: Africa’s Talking API

B. Project Schedule

Task	Duration(Months)
Project Planning	2
Requirement Gathering	3
System Design	3
Development	4
Testing and Quality Assurance	2
Deployment	2
Total	14

C. Project Budget

Item	Cost(Ksh.)
Developers	2 Million
Software Licenses	1 Million
Training	0.78 Million
Maintenance	0.8 Million
Miscellaneous	0.6 Million
Total	5.18 Million

QUOTE

“You can’t allow tradition to get in the way of innovation. There’s a need to respect the past, but it is a mistake to revere your past.”

Bob Iger(born 1951), Media Executive and Businessman

THE END