**SMART ID SCANNING SYSTEM WITH SECURITY AND DATA ANALYTICS FOR CTU DAANBANTAYAN CAMPUS**

A Capstone Project Presented to

Information Technology Department

Cebu Technological University – Daanbantayan Campus

In Partial Fulfillment of the Requirements

for the degree Bachelor of Science in Information Technology

By

Amag, Joshein

Baslan, Deonan Leo D.

Canete, Reil

Conde, Siara Lee

Coyoca, Angelica Joy

Diaga, Judy Ann

Valiente, Nin Kylle

September 2025

**TABLE OF CONTENT**

Title Page ...........................................................................................................................i

Table of Contents ..............................................................................................................ii

List of Figures ...................................................................................................................v

**CHAPTER 1: THE PROBLEM AND ITS SCOPE**

Rationale ...........................................................................................................................1

Review of Related Literature and System ........................................................................5

Technical Background ......................................................................................................8

Statement of the Problem ...............................................................................................11

Scope and Limitation of the Project ................................................................................12

Significance of the Study and Project Highlights ............................................................14

Methodology ...................................................................................................................17

Environment ...................................................................................................................17

Locale .............................................................................................................................17

Organizational Chart ......................................................................................................20

Requirements Specifications .........................................................................................21

Operational Feasibility ...................................................................................................21

Fishbone .......................................................................................................................21

Functional Decomposition Diagram ..............................................................................22

Technical Feasibility ......................................................................................................23

Schedule Feasibility .......................................................................................................24

Gantt Chart ....................................................................................................................24

Requirements Modelling ................................................................................................25

Input-Process-Output Diagram ......................................................................................25

Data and Process Modelling ..........................................................................................26

Data Flow Diagram .........................................................................................................27

System Flowchart ...........................................................................................................28

Use Case Diagram .........................................................................................................29

Class Diagram ................................................................................................................30

Design Phase ................................................................................................................31

Output and User Interface Design .................................................................................31

Reports ...........................................................................................................................32

Data Design ....................................................................................................................33

Entity Relationship Diagram ...........................................................................................33

Data Dictionary ............................................................................................................34

System Architecture .....................................................................................................36

Network Topology ........................................................................................................36

Security .......................................................................................................................36

Development Phase ....................................................................................................37

Software Specification .................................................................................................37

Hardware Specification ................................................................................................38

Program Specification ..................................................................................................39

Programming Environment ..........................................................................................39

Deployment Diagram ...................................................................................................40

Test Plan ......................................................................................................................41

Testing Phase ..............................................................................................................42

Unit Testing ..................................................................................................................43

Integration Testing .......................................................................................................43

System Testing ............................................................................................................44

Acceptance Testing ......................................................................................................44

Definition of Terms .......................................................................................................45

Ethical Considerations ...................................................................................................45

**Chapter 1**

**THE PROBLEM AND ITS SCOPE**

**INTRODUCTION**

**Rationale of the Project**

Amid rising concerns about campus safety and administrative efficiency, Cebu Technological University Daanbantayan Campus plays an important role in implementing innovative solutions to improve data management and security. The current manual ID checking process on campus are prone to errors and time-consuming, posing threats to both safety and operational efficiency. The proposed Smart ID Scanning System uses advanced scanning technology, security measures, and data analysis to streamline ID verification, improve campus security, and provide useful information of entry and exit patterns through real-time monitoring and analysis.

The lack of a digital ID verification at Cebu Technological University’s Daanbantayan Campus leads to inefficiencies and security issues, as security personnel depend exclusively on manual ID checks. However, Papesh (2018) highlights that manual ID verification is frequently slow and inaccurate, reflecting the difficulties with the campus's current practice. Similarly, Bhat et al. (2023) highlight that the lack of integrated data analytics in campus security systems restricts administrators’ capacity to make informed decisions. These deficiencies underscore the need for a technological solution to improve safety and operational efficiency. The suggested Smart ID Scanning System addresses these issues by automating the verification process and utilizing data analytics to provide useful insights.

Addressing the inefficiencies and security threats linked to manual ID verification at Cebu Technological University (CTU) Daanbantayan Campus is essential for preserving a secure and efficient learning environment. Turcu et al. (2018) highlight that outdated manual ID verification methods in educational settings increase the probability of unauthorized access, risking the safety of both students and staff. Developing a Smart ID Scanning System is crucial for delivering real-time oversight and analytical insights, as emphasized by Peng (2023), who points out the importance of analytics in enhancing campus functions. Students, staff, and administrators will gain from improved safety and more efficient access management. The results of this study will promote a more secure campus and aid in data-driven administrative choices.

The Smart ID Scanning System at Cebu Technological University (CTU) Daanbantayan Campus aligns with the broader goal of advancing educational environments through innovative technology and data-driven decision-making. By integrating automated ID verification and analytics, the study supports the development of smart campuses, as advocated by Velasco (2023), who highlights technology’s role in modernizing academic institutions. The research’s practical impact includes enhanced campus security and streamlined administrative processes, benefiting students, faculty, and staff. Theoretically, it contributes to the growing field of educational data analytics, with Zimmerman (2023) noting the potential of such systems to inform institutional policies. This study paves the way for scalable, technology-enhanced solutions in higher education settings.

**Review of Related Literature and Systems**

The use of advanced campus ID systems has become essential for enhancing security and streamlining operations in higher education institutions. Nguyen et al. (2023) highlighted that QR code–based identity systems, such as those enabling students to access campus facilities via smartphones, significantly reduce the risks associated with traditional physical ID cards. Moreover, these systems allow for real-time data collection and analytics, which provide administrators with insights to improve campus management and security measures. Therefore, integrating a Smart ID Scanning System with data analytics could enhance security protocols and modernize the campus experience for both students and staff.

The use of QR codes for identification and security has grown significantly as institutions move toward cost-efficient and reliable alternatives to traditional RFID and biometric systems. Moreover, QR codes provide a lightweight, mobile-friendly, and software-driven approach, making them highly adaptable for academic and organizational settings.

Nguyen et al. (2023) proposed an edge-computing-based entry control system using QR codes, highlighting privacy protection and efficient management through real-time data analytics in access control environments. Similarly, this aligns with the need for security and data processing in campus systems. Likewise, Kalyani et al. (2025) developed a blockchain-based personal identity security system that leverages QR codes to safeguard personal identifiable information, addressing risks of identity fraud.

In academic attendance management, QR codes have been widely studied. For instance, Aziz and Hafit (2024) discussed their application in student attendance monitoring, where QR scanning facilitated automated record-keeping and improved efficiency. Furthermore, Jaisabarish and Nimala (2024) integrated security analytics into scanning systems, demonstrating how data logs from QR scans can support vulnerability detection and predictive analysis.

Prokipchuk, Vysotska, and Nazarkevych (2024) extended QR code use by combining it with blockchain for data authentication and verification, ensuring the scanned information remains tamper-proof. In the same way, Karmoker et al. (2024) also introduced QR and blockchain integration for supply chain transparency, reinforcing that the technology is adaptable for identity validation in institutional contexts.

In healthcare and monitoring applications, Chandrasekaran and Pragadeswaran (2025) designed QR-driven systems for medicine tracking, integrating automated alerts and analytics for safety and security. Consequently, this demonstrates the versatility of QR systems beyond commercial contexts. Additionally, Dong et al. (2025) provided a survey on internet scan source identification, emphasizing the role of scan intelligence and data analytics in recognizing potential threats—important for ensuring that QR-based identity systems are not exploited.

Other supporting works include Gojanović (2024), who studied digital wallets and contactless identity systems, showing parallels in data transfer and security to QR-based ID systems. Likewise, Bolch (2024) visualized data flows for security scanning, useful for analyzing QR scan logs in real-time analytics dashboards.

Collectively, these studies highlight how QR codes serve as effective, software-driven tools for identity scanning. Therefore, they ensure security, data integrity, and actionable analytics without reliance on costly hardware such as RFID.

**Technical Background**

Information security principles serve as the foundation for the Smart ID Scanning System, which guarantees the safety of private student information. User authentication procedures guard against unwanted access, while encryption techniques preserve the secrecy of data while it is being transmitted and stored. Information security theories that are well-established and essential in academic settings are reflected in these procedures. Strong safeguards are put in place to encourage trust, dependability, and compliance.

The project's database management system is based on MySQL, a relational database management system that is ideal for storing and retrieving massive amounts of access logs and student records. The system is capable of effectively executing complex queries in real time through the use of structured query language (SQL). This guarantees that the system can manage large transaction volumes, which makes it dependable for applications involving attendance and security.

Data analytics principles provide the foundation of the system's ability to produce operational insights. While descriptive analytics provide an overview of student attendance patterns, statistical approaches aid in the identification of trends, such as peak entry and exit times. These revelations give campus administrators useful information for making decisions, like allocating resources or staffing optimally. Proactive campus management is aided by predictive analysis, which guarantees conformity with modern administrative procedures.

The system makes use of the html5-qrcode JavaScript framework for QR code reading, which enables the decoding of student IDs using smartphones or regular webcams. This cross-platform capability guarantees usability and accessibility. With the use of HTML, CSS, JavaScript, and Bootstrap, the frontend provides admins with a responsive and intuitive dashboard. The interface makes monitoring effective and simple by offering real-time visualizations of system performance, security warnings, and attendance data.

The system is powered by PHP on the server side, which controls analytics processing, database operations, and verification. The smooth interaction between PHP and MySQL guarantees dependable and safe server-side functionality. JSON Web Tokens (JWT) or session-based authentication can be used to verify users and protect data transmission from interception in order to improve security.

The dependability of QR code operations is improved by additional cryptographic concepts. For instance, Reed-Solomon error correction guarantees precise QR code decoding even in adverse scanning conditions, and AES encryption can be used to safeguard encoded student data. Analysis of entry and exit trends is done using statistical techniques like mean and frequency distributions.

The effectiveness of QR codes in academic settings has been established by earlier studies. At Sorsogon State University, Agripa and Astillero (2022) installed a QR-based attendance system, which demonstrated notable gains in lowering manual errors and speeding up attendance reporting. But their strategy lacked strong security measures and sophisticated analytics. By incorporating data analytics and more robust encryption techniques, the current system overcomes these drawbacks and becomes more in line with institutional security and management requirements.

Finally, by automating entry/exit recording, producing trustworthy academic records, and facilitating data-driven decision-making, the Smart ID Scanning System improves campus security and administrative effectiveness. Its scalable design provides a safe and long-lasting solution for resource management and student identification, supporting CTU's smart campus objectives.

**THE PROBLEM**

**Statement of the Problem**

Cebu Technological University (CTU) Daanbantayan Campus relies on manual logbooks and basic ID cards for entry and exit, leading to inefficiencies, errors, and security risks. The proposed ID Scanning System Using QR Codes, operating locally without internet reliance, aims to enhance efficiency, security, and organization. It uses QR codes for rapid, contactless user verification by role, department, course, and year/section. Integrated data analytics provide actionable insights via dashboards, supporting administrative decisions. The offline design ensures reliability within the campus’s limited network infrastructure.

Specifically, the students and staff seek to answer the following:

1. What is the demographic profile of individuals registered in the ID Scanning System as to:
   1. role in ctu community?
      1. student;
      2. staff; and
      3. faculty?
   2. department;
   3. program;
   4. year level and section?
2. What are the functional capabilities of the ID Scanning System in terms of:
   1. system accessibility and ease of use;
   2. speed and accuracy of ID recognition; and
   3. real-time recording and retrieval of attendance data?
3. What are the perceived benefits of the Local ID Scanning System among users in terms of:
   1. campus security and monitoring;
   2. time-saving and convenience; and
   3. reduction of manual processes?
4. What are the challenges in implementing the Local ID Scanning System at CTU Daanbantayan Campus as to:
5. connectivity:

4.1 network infrastructure; and

4.2 system availability and reliability;

B. compatibility and data handling:

4.3 compatibility with existing systems; and

4.4 secure storage and management of scanned data?

1. Based on the findings above, what recommendations can be proposed for enhancing the Local ID Scanning System for sustainability and effective implementation at CTU Daanbantayan Campus?

**Scope and Limitations of the Project**

**Scope of the Project**

This study focuses on developing a Smart ID Scanning System to improve campus security at CTU Daanbantayan Campus. Its goal is to deliver data-driven insights into student behaviors by leveraging modern identifying technology. The project aims to improve surveillance of campus access and entry/exit points. The method will assist both administration and students by increasing safety. The Smart ID system will include ID verification capabilities via QR code or other digital means. It will enable real-time database integration, resulting in accurate and up-to-date records. This ensures a secure and responsible tracking system.

Additionally, the system will include data analytics to monitor attendance and activity trends. It will help detect patterns such as peak hours, frequency of visits, and unusual behavior. These insights will support better campus planning and decision-making. An organized and responsive environment is expected as a result.

A visual dashboard will be created to display all relevant data in an easy-to-understand format. It will include charts, tables, and key metrics related to student movement. Staff will use this dashboard to evaluate attendance. This visual representation enhances understanding and communication of data insights.

Finally, the system will be evaluated based on its effect on security and campus operations. Feedback will be gathered from students, faculty, and staff to assess user experience. Their input will guide system improvements and future upgrades. This ensures the Smart ID Scanning System meets the real needs of the campus community.

**Limitation of the System**

The Smart ID Scanning System will be limited to implementation only at CTU Daanbantayan Campus. It will not be extended to other CTU branches or satellite campuses. This restriction is due to the scope and resources allocated for this specific study. Broader deployment may be considered in future expansions.

The system will support only university-issued IDs and will not accommodate third-party or external identification. It is designed specifically to work with CTU-generated student and staff credentials. Additionally, it will only analyze entry and exit data at monitored access points. It will not track student movements within campus facilities or classrooms.

The focus of the system is on improving security and tracking attendance, excluding features like handling tuition fees, fines, or other financial transactions. Evaluation of the system’s performance will rely on feedback collected from a selected sample group of students and staff. This may limit the overall representation of campus-wide opinions. However, it provides enough data to assess the system’s basic functionality and effectiveness.

**Significance of the Study and Project Highlights**

The Smart ID Scanning System with Security and Data Analytics at CTU Daanbantayan Campus is highly significant in enhancing campus security, improving operational efficiency, and ensuring a safer learning environment. Benefiting from this study are the various sectors as follows:

**University Administration.** This system strengthens security by ensuring that only authorized students, faculty, and staff can enter the campus. By requiring ID scans at entry points, it prevents unauthorized access, reduces security threats, and helps maintain peace and order. It also aids in monitoring attendance patterns and campus population density. These insights help the administration make informed decisions regarding campus operations and safety protocols.

**Students and Staff.** The system provides a safer and more organized environment by preventing unauthorized individuals from entering the campus. It also reduces theft and the unauthorized use of school resources, promoting accountability and security. Students and staff will feel more secure knowing that access is strictly controlled. This contributes to a more focused and peaceful learning and working atmosphere.

**Security Personnel.** The automated ID scanning process improves efficiency in monitoring campus access, making it easier to detect suspicious activities and unauthorized entries. The system enables a proactive approach to security by providing real-time insights into campus movements and peak hours. It reduces the manual burden on security personnel. They can now focus more on active patrolling and emergency response.

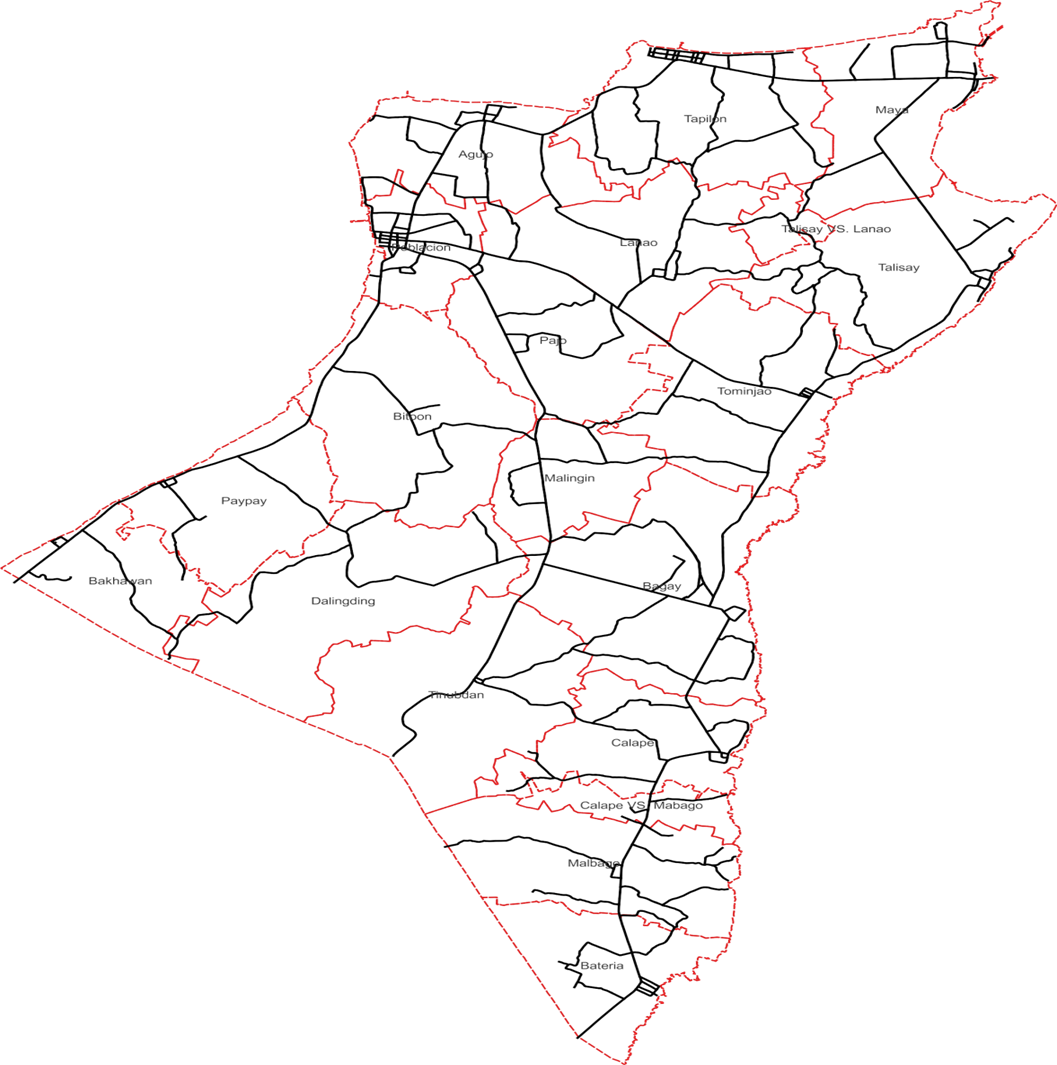
**Future Researchers.** This study serves as a reference for the development of intelligent security systems in educational institutions. It offers insights into integrating smart ID scanning with data analytics, paving the way for future advancements in campus security technology. It also identifies key challenges in implementation, such as system limitations and user adoption. Future researchers can use this study as a foundation for creating more advanced, scalable security solutions.

**Methodology**

**Environment**

**Locale**

Figure 1, shows the map of the Municipality of Daanbantayan. The locale of this study is in Cebu Technological University-Daanbantayan Campus which is located at Agujo, Daanbantayan, Cebu in which CTU is under the district 4 Divison of Cebu Province that’s within the Region VII in the Central Visayas area.



C:\Users\user\Downloads\9220651.png

**Legend**

Roads

Barangay

Boundary

Respondent’s

Location

C:\Users\user\Downloads\9220651.png

**Figure 1. Locale of the study** (CTU-Daanbantayan Campus)

The study is conducted at Cebu Technological University – Daanbantayan Campus, specifically targeting the campus entry points where the Smart ID Scanning System is implemented. The location was chosen to assess the system’s effectiveness in a real-world setting, focusing on monitoring and controlling student access.

The system will be used at the campus gates to watch and control who goes in and out. The goal is to stop people who are not students from entering the campus. The map helps us see the campus and where the main entry points are. These places will be where the Smart ID Scanning System is set up.

Around the campus, there are places like Kandaya Beach Resort, Inday Lisa Beach Resort, Skip Beach Resort, and Escalona Beach Resort. Because there are many people coming and going nearby, it is important to have a way to check if the person entering is a student or not. Since many people visit these places, more people might pass near the campus. This makes the Smart ID Scanning System even more needed which helps keep the campus safe.

**Organizational Chart**

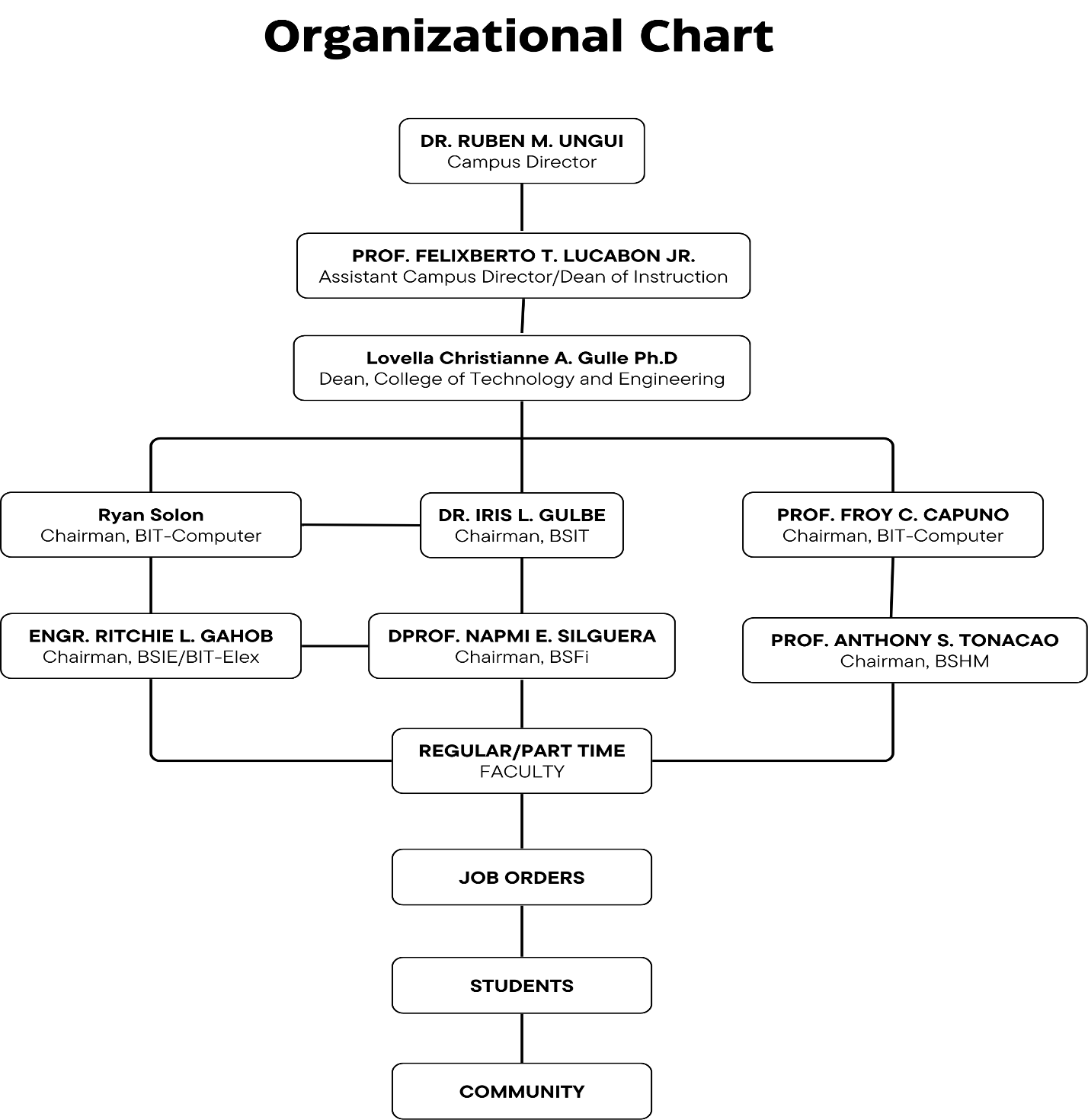


Figure 2. College of Technology and Engineering Organization Chart

**Requirements Specifications**

**Operational Feasibility**

Operational feasibility examines the practicality of implementing the Smart ID Scanning with Security and Data Analytics system for CTU Daanbantayan Campus within the university's existing infrastructure. It evaluates whether current resources, staff, and processes can support and maintain the system's advanced scanning capabilities, security protocols, and data analytics functions. Ensuring this feasibility is crucial for the system's long-term sustainability, security enhancements, and effective data-driven decision-making.

**Fishbone**

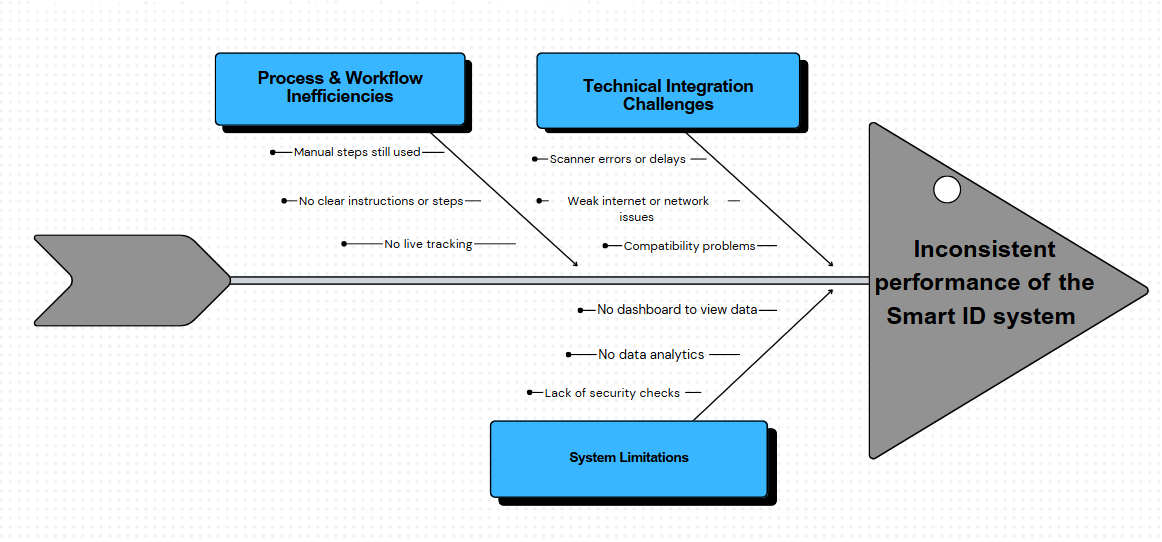
Figure 3, The fishbone diagram illustrates the main factors contributing to the inconsistent performance of the Smart ID system. These factors are grouped into technical integration challenges, process and workflow inefficiencies, and system limitations, all of which affect the reliability and efficiency of the system.

Figure 3. Fishbone Diagram

Technical integration challenges include scanner errors or delays, weak network connectivity, and compatibility issues, which hinder smooth operation. Workflow inefficiencies, particularly the lack of live tracking, reduce the effectiveness of monitoring and verification. System limitations, such as slow response times, limited data storage, and insufficient security checks, further impact performance. Together, these issues explain the overall inconsistencies observed in the Smart ID system.

**Functional Decomposition Diagram**

Figure 4, The diagram illustrates the structure and key components of the Smart ID Scanning System with Security and Data Analytics. It highlights the main modules, including ID Scanning and Verification, User Management and Security, Data Management, Analytics and Reporting, and System Administration. Each module is broken down into specific functions that ensure the system operates efficiently and securely.

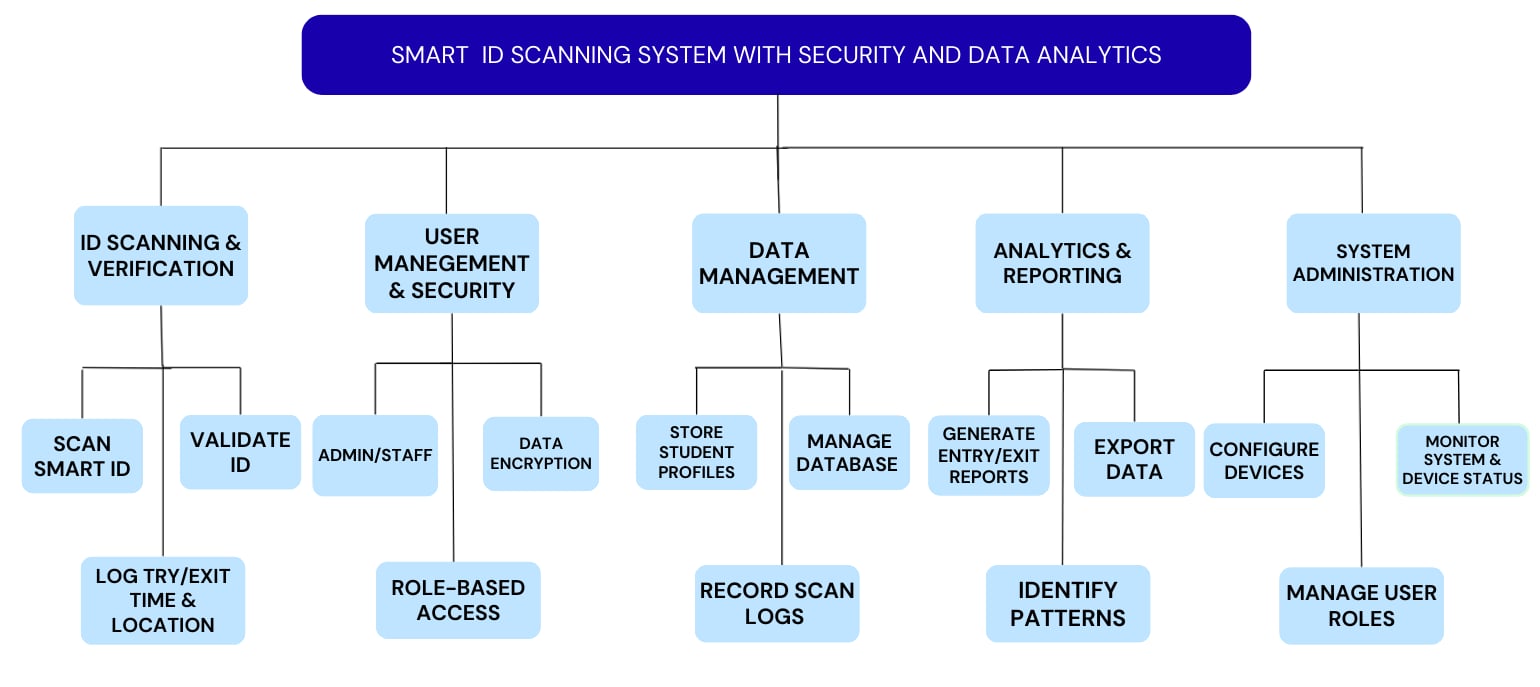


Figure 4. Functional Decomposition Diagram

The ID Scanning and Verification module handles scanning, validating IDs, and logging entry and exit times and locations. User Management and Security includes admin or staff login, role-based access, and data encryption. Data Management covers storing student profiles, managing databases, and recording scan logs. Analytics and Reporting focuses on generating reports, exporting data, and identifying patterns. System Administration manages device configuration, monitoring, and user roles.

Together, these components demonstrate how the system integrates security, data management, and analytics to streamline campus ID verification processes.

**Technical Feasibility**

The technical feasibility of the project "Smart ID Scanning with Security and Data Analytics for CTU Daanbantayan Campus" appears promising, considering the availability of modern scanning technology and data analytics tools. With qualified technical staff and adequate infrastructure in place, incorporating features such as ID scanning, real-time security monitoring, and data analytics for campus safety appears feasible. Ensuring interoperability with existing campus devices and systems, as well as including robust security measures, will be critical considerations for a smooth and secure user experience. Furthermore, utilizing scalable designs and advanced analytics solutions can improve performance while accommodating future enhancements and advancements in security technology.

**Schedule Feasibility**

**Smart ID Scanning System with Security and Data Analytics for CTU Daanbantayan Campus**

Figure 5. Gantt Chart

Figure 5, The Gantt chart shows the various task involved in creating the Smart ID Scanning system for CTU Daanbantayan Campus, as well as their timelines. Each task is represented by a horizontal bar, the length of which corresponds to the task’s time. The chart visualizes the project schedule, allowing researchers to track progress, manage dependencies, and guarantee that each task is completed on time.

**Requirements Modeling**

**Input-Process-Output Diagram**

In Figure 6, The flow diagram illustrates the Smart ID system, organized into three main stages: Input, Process, and Output. The Input stage collects Smart ID data, user credentials, and profile information such as name, program, and role, providing the necessary information for verification and access control.

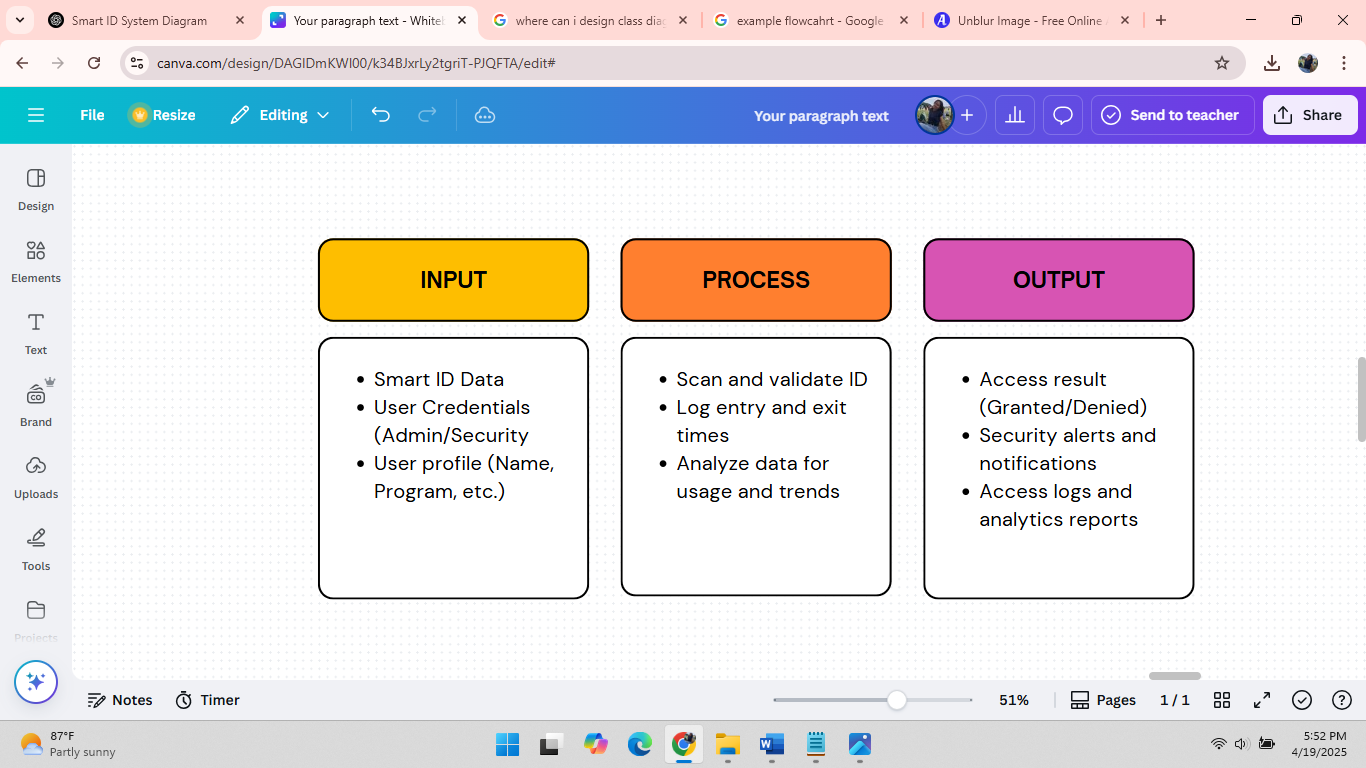


Figure 6. Input-Process-Output Diagram

In the Process stage, the system scans and validates IDs, logs entry and exit times, and analyzes data to identify usage patterns and potential anomalies. The Output stage delivers access results, security alerts, notifications, and comprehensive access logs with analytics reports. The diagram demonstrates how information flows from user input through processing to actionable outputs, ensuring secure and efficient campus operations.

**Data Flow Diagram**

Figure 7, The Data Flow Diagram illustrates how information moves within the Smart ID scanning system. Users, including students, staff, and visitors, interact with the system to generate access results, which indicate whether entry is granted or denied.

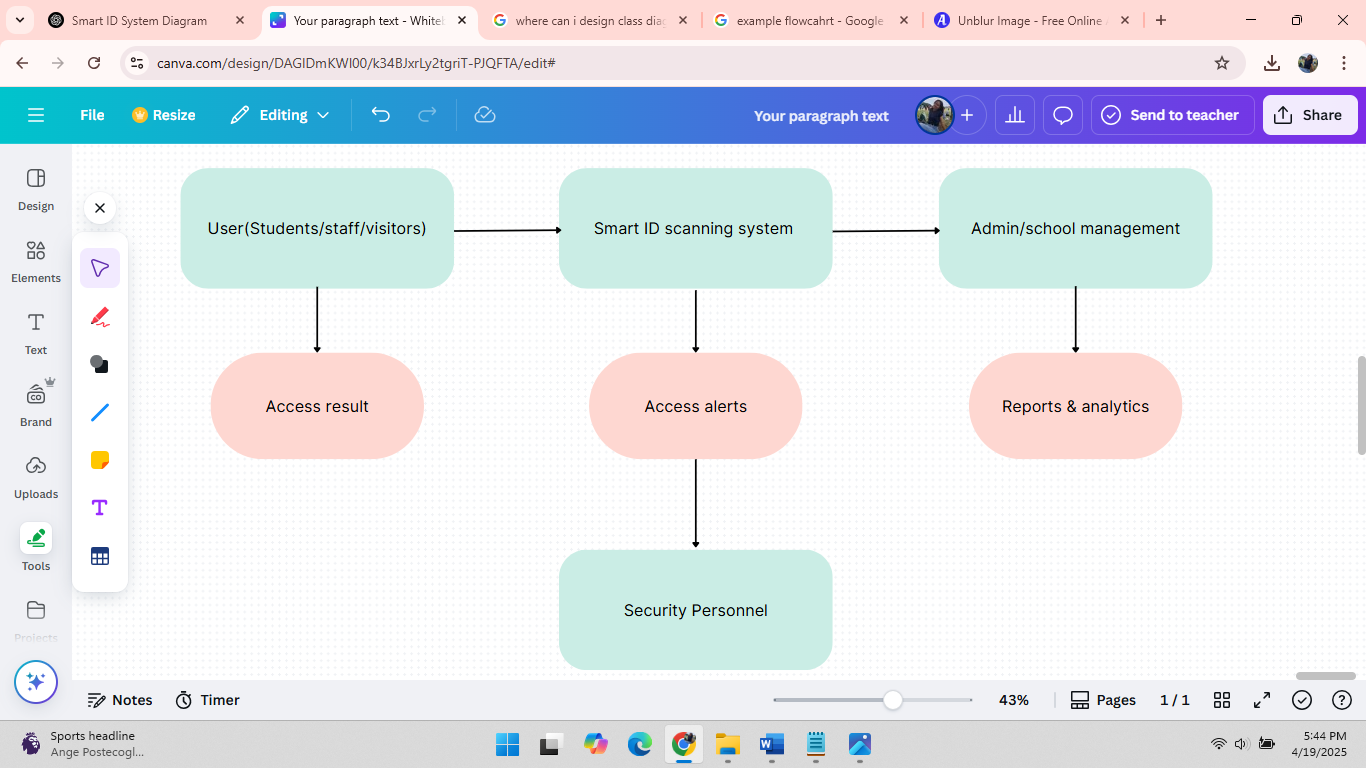


Figure 7. Data Flow Diagram

The system also produces access alerts directed to security personnel, allowing them to respond to unauthorized attempts or unusual activity. Additionally, the Smart ID scanning system communicates with admin or school management to provide reports and analytics, helping administrators monitor overall campus access and activity trends. The diagram visually summarizes the flow of data from users to processing, security monitoring, and administrative reporting.

**System Flowchart**

Figure 8, The Smart ID Scanning System follows a step-by-step process to ensure and efficient entry into the campus. The process begins when a user approaches the scanning station.

Figure 8. System Flowchart

At this point the system prompts the user to scan their smart ID. After scanning, the system automatically checks whether the scanned ID is registered in the database. If the ID is found in the database, the system grants access to the user and logs their entry into the system for record-keeping purposes. If the ID is not registered, the system denies access and automatically alerts the campus security personnel about the attempt.

After logging the entry of registered users, the system proceeds to determine whether the individual is a visitor. If the user is not a visitor, the process continues normally and the individual may proceed to enter the campus. On the other hand, if the user is identified as a visitor, the system immediately records their visit by logging the necessary details into the database. In this version of the system, there is no separate validation step for visitor information, allowing for a more streamlined entry process.

Once all entry data has been collected, the system send the information to the analytics tool. The tool is responsible for generating reports that show campus access patterns, attendance, and other relevant data. These reports are then used by the administrators and security personnel to support campus safety, monitor activities, and make informed decisions. The process ends after all after data has been processed and recorded by the system.

**Object Modelling**

**Use Case Diagram**

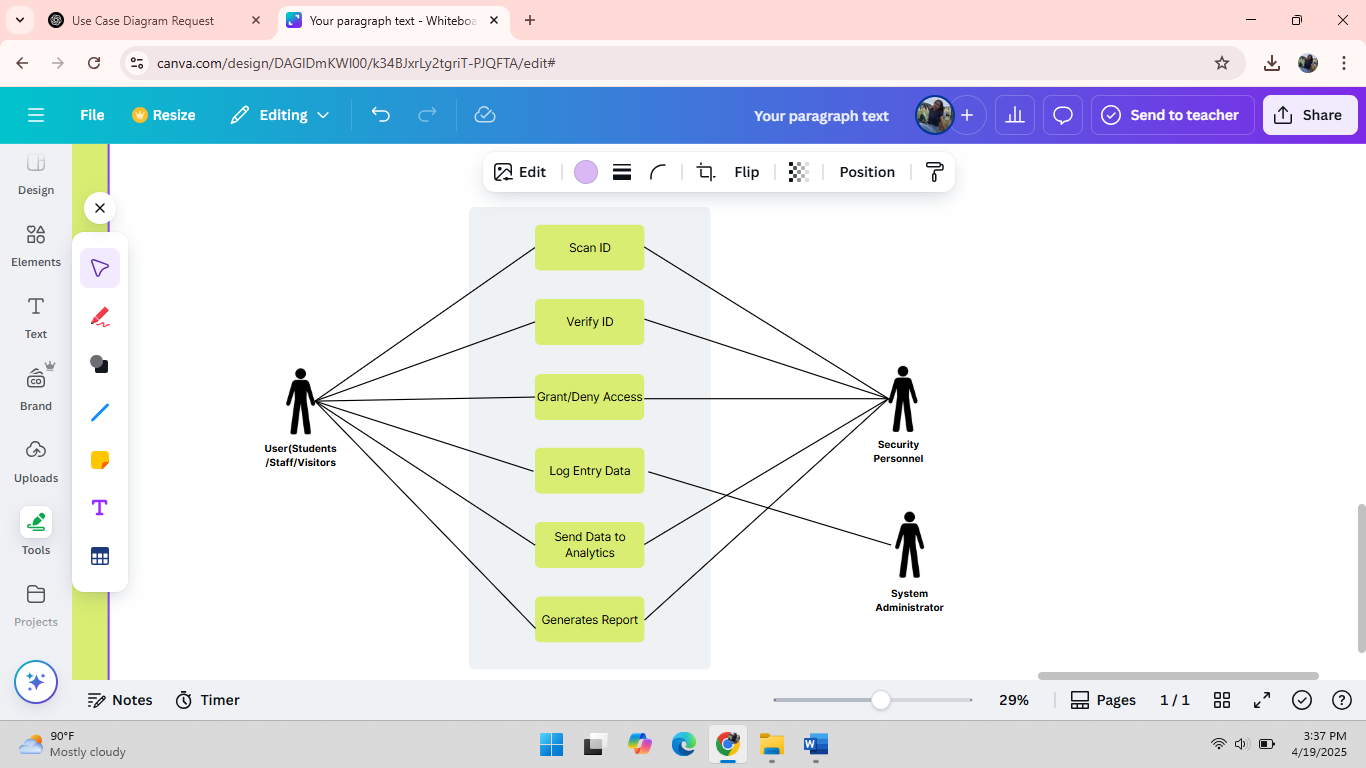
Figure 9, the use case diagram shows how different people interact with the Smart ID Scanning System. It highlights the main tasks each person can do in the system.

Figure 9. Use Case Diagram

Users like students, staff, and visitors can easily scan their Smart IDs to enter the campus. The system checks if the ID is valid, then either allows or denies access. If access is granted the system records the entry. If someone tries to enter with an unregistered ID, the system alerts the security personnel. The system also sends entry data for analysis. Meanwhile, the system administrator can manage user data, monitor the system, and generate reports for better decision making.

**Class Diagram**

Figure 10, the class diagram represents the structure of the system, showing how the different classes interact to manage and monitor campus access securely and efficiently.

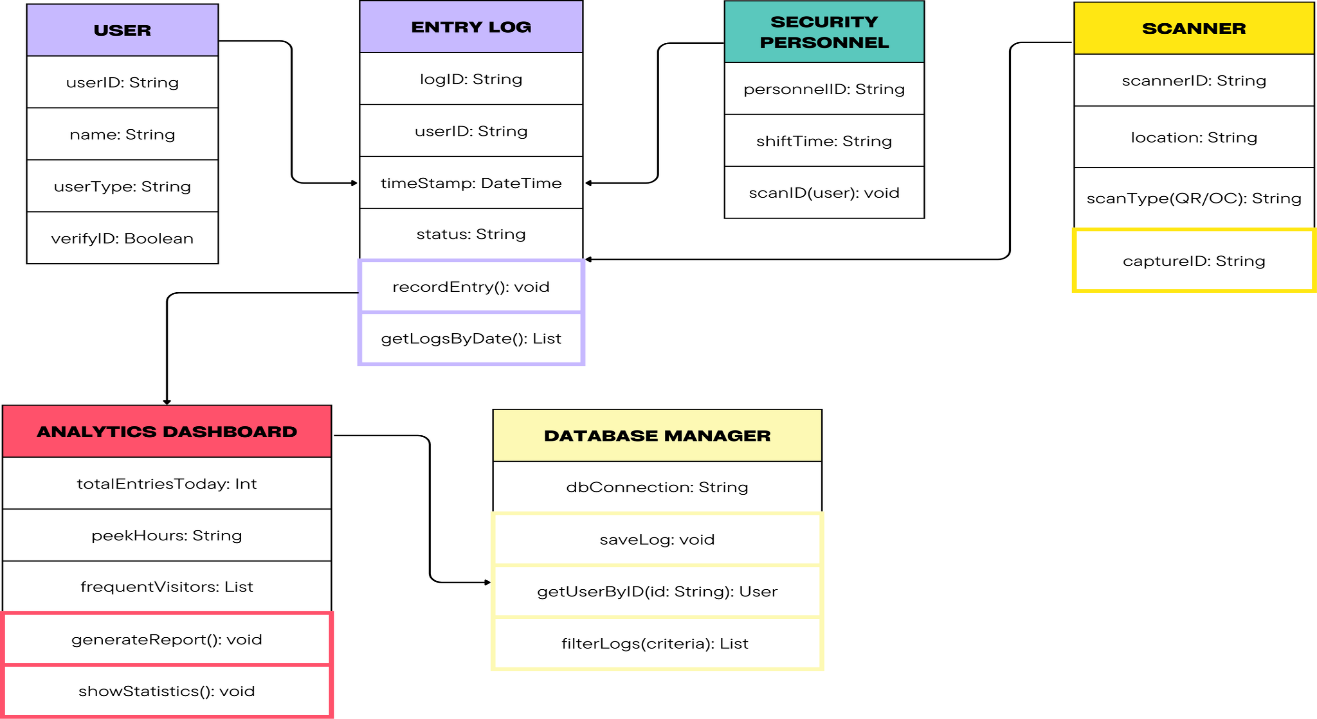


Figure 10. Class Diagram

The main components of this system include user, security personnel, scanner, entry log, analytics dashboard, and database manager. Each user, such as student or staff member, is verified by scanning their ID, which is handled by the security personnel using a scanner device. Every entry or exit is recorded in the entry log with details such as the timestamp and status. These logs are saved and managed through a central database. The system also includes an analytics dashboard that processes and presents important data like the total number of entries for the day, the busiest times (peak hours), and the most frequent visitors. Overall, the class diagram helps visualize how the system supports campus safety, improves monitoring, and provides valuable insights for administrative decision-making.

**DESIGN PHASE**

**Output and User Interface Design**

**Reports**

The system generates reports to help administrators monitor campus access and identify patterns. The Daily Gate Traffic Report shows entries and exits by hour, highlighting busy periods. The Individual Entry/Exit History Report tracks a person’s movements over a selected period for security checks. The Visitor Log Report records daily visitor details, including purpose and meetings. The Gate Traffic Insights Report uses analytics to reveal trends, helping optimize staffing and security.

**Data Design**

The data design organizes all the information the system collects. The Person Table stores details of students, staff, and visitors: ID number unique, full name, role student, staff, or visitor, contact number, and QR code data. The Entry/Exit Table logs every gate movement, linking the person’s ID number, date, time, direction entry or exit, and gate. The Visitor Table holds additional visitor details: visitor ID, name, contact number, purpose, person they’re meeting, and temporary QR code data. To keep data secure, QR codes are encrypted, and only authorized staff can access the system with a password. It also has a Data Analytics where administrator and security staff can view the Web Dashboard to track patterns, peak hours, attendance etc. The system also backs up data regularly to prevent loss.

**Entity Relationship Diagram**

Figure 11, An Entity Relationship Diagram visually maps out the structure of a database, showing how data is organized and related. In our Smart ID Scanning System for CTU Daanbantayan, the ERD defines the tables, their attributes, and relationships to track entry/exit using QR codes on devices like tablets or any device with a built-in camera, while enabling data analytics for campus security and insights.

Figure 11. Entity Relationship Diagram

The diagram shows that each table can access and interact with relevant data to manage the system effectively. Additionally, it highlights the relationships between entities, such as the association between the Person Table and Entry/Exit Table for tracking individuals, and the connection between the Analytics Table and Entry/Exit Table for generating insights.

**Data Dictionary**

|  |  |  |
| --- | --- | --- |
| Variable Name | Data Type | Description |
| Person Table |  |  |
| ID\_Number | VARCHAR | Unique ID for each person |
| FullName | VARCHAR | Person's complete name |
| Role | VARCHAR | Role of the person (e.g., Student, Staff) |
| Contact\_Number | VARCHAR | Phone number of the person |
| QR\_Code\_Data | TEXT | Data encoded in QR code |
| Entry/Exit Table |  |  |
| Event\_ID | INT | Unique ID for each entry/exit event |
| ID\_Number | VARCHAR | Linked to person ID |
| Date | DATE | Date of event |
| Time | TIME | Time of event |
| Direction | VARCHAR | Entry or Exit |
| Scanner\_ID | VARCHAR | Linked to Scanner table |
| Visitor Table |  |  |
| Visitor\_ID | INT | Unique ID for each visitor |
| Name | VARCHAR | Visitor's name |
| Contact\_Number | VARCHAR | Visitor's contact number |
| Purpose\_of\_Visit | TEXT | Reason for visiting |
| Person\_to\_Meet | VARCHAR | Name of person the visitor wants to meet |
| Analytics Table |  |  |
| Analytics\_ID | INT | Unique ID for analytics record |
| Date | DATE | Date of the analytics summary |
| Scanner\_ID | VARCHAR | Linked to Scanner table |
| Total\_Entries | INT | Number of entries |
| Total\_Exits | INT | Number of exits |

|  |  |  |
| --- | --- | --- |
| Peak\_Entry\_Time | TIME | Time with highest entries |
| Peak\_Exit\_Time | TIME | Time with highest exits |
| Scanner Table |  |  |
| Scanner\_ID | VARCHAR | Unique scanner device ID |
| Admin Table |  |  |
| Admin\_ID | INT | Unique ID for admin |
| Full\_Name | VARCHAR | Admin's full name |
| Username | VARCHAR | Admin's login username |
| Password | VARCHAR | Admin's password |
| Contact\_Number | VARCHAR | Admin's contact number |
| Security Table |  |  |
| Security\_ID | INT | Unique ID for security personnel |
| Full\_Name | VARCHAR | Security personnel's name |
| Username | VARCHAR | Login username for security |
| Password | VARCHAR | Login password for security |
| Contact\_Number | VARCHAR | Security contact number |
| Scanner\_ID | VARCHAR | Linked to assigned scanner |

This comprehensive database schema includes multiple interconnected tables, each designed to store specific types of information relevant to the institution's entry monitoring, personnel, and security operations. By organizing data into distinct tables like Person, Entry/Exit, Visitor, Analytics, Scanner, Admin, and Security, the system ensures structured and efficient data management, facilitating accurate tracking and secure access control.

The Person table stores the identification, contact details, role, and QR code data of individuals affiliated with the institution. The Entry/Exit table logs entry and exit events, associating them with specific persons and scanners, including timestamps and direction of movement. The Visitor table captures visitor information such as name, contact number, purpose of visit, and whom they intend to meet.

The Analytics table summarizes daily traffic statistics per scanner, including total entries and exits, as well as peak times. The Scanner table holds unique identifiers for scanning devices used throughout the campus. The Admin table secures administrator credentials and contact details, while the Security table stores security personnel profiles and their assigned scanner devices.

This structured schema enhances operational efficiency, security monitoring, and data accessibility. It supports streamlined movement tracking and informed decision-making through analytics, contributing to a safe and well-organized institutional environment.

**System Architecture**

Scalability, modularity, and security are key components of the Smart ID Scanning with Security and Data Analytics system architecture for CTU Daanbantayan Campus. To guarantee adaptability, maintainability, and future scalability, it has a tiered architecture that divides the database, application logic, and user interface layers. Real-time scanning, user verification, data recording, and analytics reporting are all handled effectively by the system. It enables smooth operations and precise tracking of people coming into and going out of the campus by integrating scanning devices at multiple access points with a secure local server and an analytics dashboard.

**Network Topology**

A dependable local server-based network topology is employed by the Smart ID Scanning System. A local area network (LAN) connects the scanning devices at the main entry and exit points, enabling quick and safe data transfer throughout the campus. To guarantee quicker access, less downtime, and greater control over campus operations, all data gathered from ID scans is processed and stored on-site servers. This localized strategy ensures that security monitoring and data logging continue unabated during network outages by removing reliance on external networks and permitting offline functionality.

**Security**

Security is a top priority for the Smart ID Scanning System. To protect user data and stop illegal access, the system employs several levels of security. It records entry and exit logs and verifies identities by scanning QR codes. Role-based login credentials for administrators and security staff regulate access to system features. Every sensitive piece of information is safely kept on the local server with restricted access. To protect the network from possible threats, the system incorporates firewall protection and uses encryption for data transmission. The system is kept in compliance with data security standards through routine maintenance and internal audits, guaranteeing the availability, confidentiality, and integrity of all records. At the CTU Daanbantayan Campus, these extensive security measures contribute to the development of a reliable and secure environment for visitors, employees, faculty, and students.

**DEVELOPMENT PHASE**

The entire cycle, from requirement analysis to deployment, is covered in the Smart ID Scanning System development phase. First, specific needs from the campus environment are gathered. Next, the system is designed, features like ID scanning and analytics are implemented, and performance and dependability are rigorously tested. Real-time reporting, data accuracy, and user experience are given particular consideration. Every module, including analytics, visitor logging, person management, and scanning, has been designed to function safely and smoothly within the CTU Daanbantayan Campus infrastructure, enhancing campus security and monitoring.

**Software Specifications**

For effective, scalable, and secure operations, the Smart ID Scanning System with Security and Data Analytics for CTU Daanbantayan Campus was created utilizing contemporary web technologies. React is used to build the frontend, giving administrators and security staff an interactive and responsive user interface. Analytics reports, system alerts, and entry and exit trends can all be seen in real time on this dashboard.

HTML5-qrcode, a JavaScript-based library that allows webcam or device camera scanning straight through the browser, handles the QR code scanning functionality. As a result, the system can be readily installed on laptops, tablets, or mobile devices without the need for external scanning hardware. Node.js and the Express framework power the backend, which manages user accounts, logs, real-time verification, and data analytics calculations. It controls communication between the database, scanning devices, and frontend, acting as the central control unit.

To guarantee safe user authentication and safeguard data transfer between the frontend, backend, and database, security is implemented using JWT (JSON Web Tokens). This aids in enforcing role-based access and guards against system abuse. The system provides CTU Daanbantayan Campus with a strong, contemporary solution for safe identity scanning, real-time monitoring, and analytics by fusing these technologies.

**Hardware Specifications**

The Smart ID Scanning with Security and Data Analytics system for CTU Daanbantayan Campus uses the following hardware components:

1. QR Code Scanning Devices: Uses standard webcams or device cameras compatible with the html5-qrcode library for real-time scanning.
2. Local Server: Equipped with a quad-core processor, 4GB RAM, and 256GB SSD for efficient data handling and backend processing.
3. Network Setup: Operates on a stable campus LAN or Wi-Fi network to ensure continuous connectivity between client devices and the server.
4. Maintenance: Regular device and system checks are performed to ensure optimal performance and reduce hardware issues.
5. Power Backup: Basic uninterruptible power supply (UPS) units are used to prevent data loss during power interruptions.

**Program Specifications**

The system is developed using a modular architecture with Node.js and Express handling backend logic and MySQL as the database. The React frontend provides a dynamic dashboard for viewing analytics and trends. The QR code scanning functionality is powered by html5-qrcode, integrated directly with device cameras. The system uses JWT (JSON Web Token) for secure user authentication and data transfer. Code is structured using standard conventions, and the architecture allows for easy maintenance, scalability, and future feature expansion.

**Programming Environment**

The system is developed using Visual Studio Code as the primary IDE. The user interface is built with HTML, CSS, and JavaScript, while Node.js and Express are used for backend development. The MySQL database manages records and logs. QR code scanning is implemented using the html5-qrcode JavaScript library. The system uses JWT for secure data transmission and authentication. This environment supports efficient coding, debugging, and modular development, with potential for future scalability.

**Deployment Diagram**

Figure 12, The Deployment Diagram illustrates how the Smart ID Scanning with Security and Data Analytics system is deployed across local infrastructure.

Figure 12. Deployment Diagram

At the top, a User Device interacts with the system through a local web interface. In the center, a Local Web Server hosts the Node.js/Express backend and the React frontend dashboard. Below that, a Local Database Server runs MySQL, storing logs, person records, and analytics data. The system also uses html5-qrcode on the user's device to scan QR codes via webcam. All components communicate over a secure local network, and JWT is used to maintain secure sessions and data transfers. This diagram reflects a fully local deployment, eliminating reliance on external cloud services for core operations.

**Test Plan**

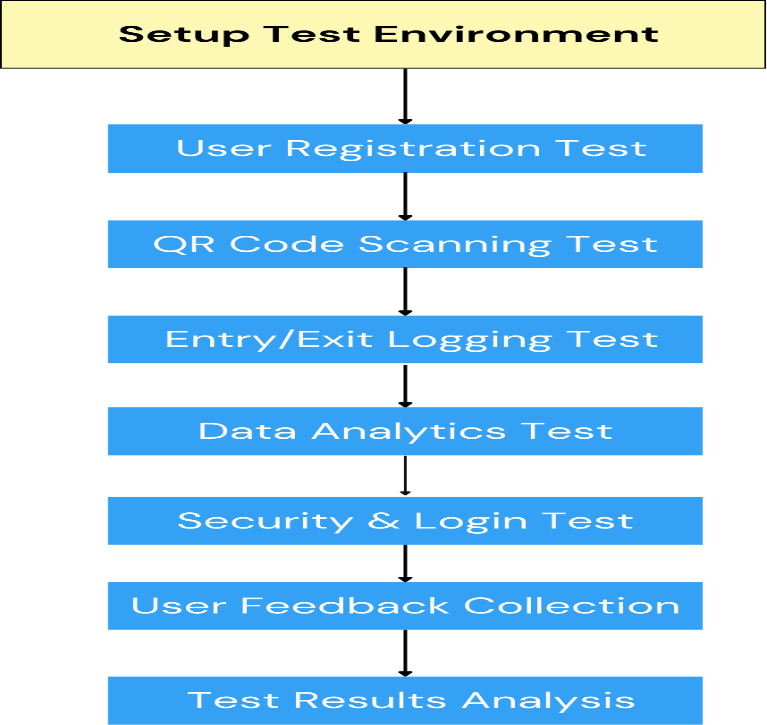
****Figure 13, this test plan outlines the steps to test the Smart ID Scanning System to ensure that it works properly, provides accurate entry and exit records, protects user data, and supports real-time analytics. The goal is to verify that the system is functional, reliable, secure, and user-friendly.

Figure 13. Test Plan

In this diagram, it illustrates the step-by-step testing process of the system. The testing starts with setting-up the environment, where all devices like scanners and laptops are prepared, and the system is installed. After that, the user registration test is done to check if the system can save user information correctly. Then, the data analytics feature is tested to see if the dashboard shows accurate reports, such as attendance and peak entry times. The next part is the QR code scanning test, where users scan their ID and the system checks if their identity is displayed properly. After that, the entry and exit logging is tested to make sure the time logs are correct and stored in the database.

The process continues with the security and login test to check if only authorized users can access system and if user data is protected. Once the test .is all completed, the team does a test result analysis to review everything that happened during the test. Finally, user feedback is collected to understand how users felt about using the system and what improvements can be made. This full testing process helps ensure that the system is working well before it is used on campus.

**TESTING PHASE**

The testing phase is important part of system development where the Smart ID Scanning System is tested to make sure all features work properly. This includes checking if users can register, scan their IDs, log their entry and exit times, and view analytics on the dashboard. Security features are also tested to make sure that only authorized users can access the system and that personal data is protected. After testing, feedback is gathered from users, and results are reviewed to find and fixed any issues. This helps ensure that the system is reliable, secure, and ready to be used at CTU – Daanbantayan Campus.

**Unit Testing**

Unit testing ensures that each part of the system like QR code scanner, login form, database connection, or dashboard panel works correctly on its own. This type of testing helps find problems early, so they can be fixed before moving on to the full system. By testing each function separately, developers can make sure everything works as expected. This leads to fewer error and a smoother user experience once the full system is complete and ready for use on campus.

**Integration Testing**

Integration testing involves checking whether the different components of the system work together correctly. This includes verifying that the QR code scanner properly sends data to the database, the login system connects to user information securely, and the dashboard accurately displays the collected data. Integration testing helps catch and resolve issues that come up when different parts of the system connect, so the whole system work without problems.

**System Testing**

System testing checks the entire Smart ID Scanning System to make sure all features work correctly together in a real environment. This testing covers everything from scanning IDs, recording entry and exit times, showing data on the dashboard, to security functions like user login and data protection. The goal is to confirm that the system meets all requirements and performs well under actual conditions before it is fully used at CTU Daanbantayan Campus.

**Acceptance Testing**

Acceptance testing is the final phase where end-users at CTU Daanbantayan Campus, including students, faculty, and security staff, evaluate the Smart ID Scanning System. This phase ensures the system meets all requirements and functions effectively in real campus operations. Key features such as QR code scanning, attendance logging, data analytics, and security controls are tested. Feedback from users helps identify any issues before full deployment. Successful acceptance testing confirms the system is ready for use to improve campus security and management.

**DEFINITION OF TERMS**

**Smart ID Scanning System –** A digital system designed to verify identity using QR codes and record entry/exit data in real time for improved campus security and operational efficiency.

**QR Code –** A machine-readable code containing information about the user, used in this system for quick and contactless ID verification.

**Data Analytics –** The process of examining collected data (e.g., entry/exit times) to identify trends, patterns, and insights for campus planning and decision-making.

**Authentication** – The process of verifying the identity of a student or staff member to ensure secure access to the campus.

**Encryption** – A method of securing data by converting it into a coded format to prevent unauthorized access during storage or transmission.

**Real-Time Monitoring** – The continuous observation and logging of campus entry/exit activities as they occur, allowing immediate action if needed.

**Database Management System (DBMS)** – A software tool used to store, retrieve, and manage student and staff records securely and efficiently.

**Dashboard** – A user interface that displays important system data such as attendance logs and peak access times in charts or tables for easy analysis.

**Node.js/Express** – Backend technologies used to build and manage the server-side functions of the ID Scanning System.

**JWT (Jason Web Tokens)** – A security mechanism used to authenticate users and maintain secure sessions within the system.

**Security Protocols** – Rules and configurations implemented in the system to protect against unauthorized access and data breaches.

**Operational Efficiency** – The system’s ability to streamline campus processes like attendance and access control with minimal time and resource usage.

**Scalability** – The capability of the system to be expanded or upgraded in the future without affecting its performance or stability.

**ETHICAL CONSIDERATIONS**

In conducting this study, the researchers made sure to follow ethical guidelines to protect the privacy, safety, and rights of the people who joined the development and testing of the Smart ID Scanning System and Data Analytics for Cebu Technological University – Daanbantayan Campus.

**Informed Consent.** All participants, such as students, teachers, and staffs, joined the study voluntarily. They were informed about the purpose of the study and what would happen. A consent form was given before any data was collected. They were free to say no or leave the study at any time without any problem.

**Confidentiality and Privacy**. The system collects personal information like names, ID numbers, departments, and courses. These details were kept private and were only seen by the researchers and authorized school staff. No personal data was shared publicly, and no names were included in the results.

**Data Protection and Security.** All the data collected was kept safe and secure using passwords and encryption. This means the information was protected so that no one without permission could access or changed it. The system also used safety tools like HTTPS and other technologies to protect user data.

**Voluntary Participation and No Harm.** Nobody was forced to join the study. The system was made to help improve security on campus and not to harm or judge anyone. It only tracks who enters or leaves the campus and does not watch what people do inside.

**Transparency and Honesty.** The researchers were honest in reporting the results. No data was changed or made up. All sources and related studies used in the project were properly credited to avoid plagiarism.

**Respect and Fairness.** All participants were treated with respect and equality. Everyone’s feedback and suggestions were appreciated and used to help improve the system.

**Use of Research Output.** The result of this research will be used to improve the school’s security and attendance system. The system may also serve as a helpful reference for future student researchers who want to build similar projects.

By following these ethical practices, the researchers made sure that the project was done in a safe, fair, and responsible way for the benefit of CTU – Daanbantayan Campus