APPLIED INFORMATION TECHNOLOGY AND COMPUTER SCIENCE
e-ISSN: 2773-5141

AITCS

Vol. 6 No. 2 (2025) 1416-1435
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

RFID-Based Vehicle Access and Monitoring System

Nur Nadhirah Masri[1], Ruhaya Ab. Aziz[1]*

[1] *Fakulti Sains Komputer dan Teknologi Maklumat,*
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

Corresponding Author: ruhaya@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2025.06.02.076

Article Info

Received: 29 July 2025
Accepted: 20 November 2025
Available online: 30 November 2025

Keywords

RFID, Object-Oriented, Prototyping Model, Vehicle Access, Monitoring System

Abstract

Radio Frequency Identification (RFID) technology uses electromagnetic fields to identify and track objects, making it an effective tool for security. This project aims to develop an RFID-Based Vehicle Access and Monitoring System to address inefficiencies, human errors, and security risks in Universiti Tun Hussein Onn Malaysia's (UTHM) current manual vehicle access system. The system is designed using an object-oriented approach and follows the prototyping model to iteratively develop the solution. It integrates RFID tags to automate vehicle access and provide real-time monitoring. The implementation includes vehicle entry points on UTHM's main campus, with a focus on operational efficiency and increased security. The expected results include reduced human error, shorter wait times at entry points, and improved data accuracy for security purposes. This study shows how automation can make campus environments safer and more efficient, and it proposes additional improvements for future systems, such as integrating statistical analysis.

1. Introduction

Radio Frequency Identification (RFID) technology uses electromagnetic fields to automatically identify and track objects, making it widely applicable in various sectors such as security, healthcare, and logistics [1]. Its ability to automate processes and provide real-time data has made RFID an increasingly popular tool for improving operational efficiency, particularly in vehicle access control systems. RFID technology has shown continued growth in several fields, including security and access management [2]. Universities, including Universiti Tun Hussein Onn Malaysia (UTHM), require an efficient and secure method to control vehicle access, ensuring the safety of students, faculty, and property while reducing delays during peak hours.

At present, UTHM's vehicle access is managed manually, with security staff checking IDs or vehicle stickers at entry points. This manual process is prone to errors, leading to security risks, delays, and traffic congestion. Additionally, the absence of real-time data and a central database makes it difficult to monitor vehicle patterns or analyze traffic management effectively.

Therefore, to address these issues, this project proposes the development of an RFID-Based Vehicle Access and Monitoring System. By automating vehicle identification, the system will reduce wait times, eliminate human error, and enhance security. Furthermore, it will generate real-time data, enabling better resource allocation and traffic management, while providing a flexible, data-driven approach to campus security.

The objectives of the project are:

I. To design an RFID-based vehicle access and monitoring system using an object-oriented approach.

II. To develop an RFID-based system that automates the process of granting or restricting vehicle access to the UTHM campus based on authorized RFID tags.

III. To test the RFID-based vehicle access and monitoring system to ensure the functionality.

The main purpose of this project is to develop and implement an RFID-based vehicle access control system designed for Universiti Tun Hussein Onn Malaysia (UTHM). The system aims to increase campus security through automation and user-friendly interfaces, expedite vehicle entry and exit procedures, and improve user and security staff experiences. The system will be specifically implemented at UTHM's main campus, covering all vehicle entry points where RFID tags are used to verify that all cars entering the campus are authorized. The system function module includes register user account, login, manage user information, manage vehicle information, manage vehicle access, monitor unauthorized access alert, and generate report, listed as shown in Table 1.

Table 1 *System Function Module*

System Module	Description
Register user account	Allows new users (security staff, staff, and student) to create accounts by entering personal information and setting up authentication details.
Login	A secure login for staff and students to access the system to register their vehicles. Features secure authentication such as username, and password.
Manage User Information	A module that allows user to update their profile in the system. Allows security staff to view all registered users, update data, and update RFID tag information.
Manage Vehicle Information	A module that allows users such as staff or students to register new vehicles, including details such as vehicle number, owner information, and associated RFID tags.
Manage Vehicle Access	Provide features to manage and monitor the access of registered vehicles, such as verifying RFID tag information and granting access based on permissions.
Monitor Unauthorized Access Alert	This module is designed to improve campus security by instantly detecting and notifying security staff of any attempts by unauthorized vehicles to access the campus. It automatically detects vehicles not registered in the system, triggering a sound alert and the system will push notifications to the security staff dashboard, and immediate alerts for manual verification and action.
Generate Report	Generates reports related to vehicle registrations and vehicle access history, providing insights for security and administrative purposes.

The system includes seven main modules that help manage vehicle access on campus. These modules allow users to register and log in, manage their personal and vehicle details, control access using RFID, detect unauthorized entry, and generate reports. Each module works together to improve security and make the system easy to use for staff and students.

2. Related Works

This section will discuss on literature review on RFID-based vehicle access and monitoring system and the comparison of similar systems.

2.1 Domain Background

Universiti Tun Hussein Onn Malaysia (UTHM) is a leading institution committed to academic excellence, innovation, and sustainability. As part of its mission to create a secure and efficient campus environment, UTHM is creating technology-driven solutions that improve safety, operational efficiency, and user convenience. The increasing number of vehicles on campus creates challenges such as traffic congestion, delays at entry points, and potential security risks from unauthorized access.

Therefore, to address these issues, UTHM requires an automated vehicle access management system that reduces human error, shortens wait times, and enhances campus safety. The proposed RFID-Based Vehicle Access and Monitoring System aligns with the university's goal of utilising advanced technologies to improve campus infrastructure and operational processes. This system aims to improve vehicle access and create a safer environment for students, staff, and visitors.

2.2 RFID-Based Vehicle Access

Managing vehicle access in controlled environments, such as campuses, is critical but challenging. Uncontrolled access invites security risks such as unauthorised entry and theft, while also causing significant traffic problems such as traffic jams, which have a direct impact on safety and efficiency. Traditional manual checks are slow and prone to errors, and some automated systems, such as license plate recognition, can be unreliable due to environmental conditions. An effective, efficient, and secure system is required to maintain order and safety in these environments.

This is where RFID (Radio Frequency Identification) technology offers an improved solution. Unlike older methods, RFID enables vehicles to pass through access points automatically and instantly, eliminating difficulties and significantly improving traffic flow. A small, secure tag attached to the vehicle communicates effortlessly with a reader, ensuring high accuracy and reliability unaffected by weather or dirt [3]. This makes RFID a highly adjustable solution for managing large numbers of vehicles. RFID systems can easily integrate with central databases, providing real-time.

The RFID-based Vehicle Access and Monitoring System utilizes a web-based platform as its primary interface for all users, including staff, students, and security staff. The system integrates RFID technology to enable efficient, contactless vehicle identification and monitoring at access gates [4]. Unauthorized access attempts trigger real-time sound alerts and notifications displayed on the security dashboard for immediate action. Data is securely stored in a centralized MySQL database, allowing real-time processing for vehicle verification, reporting, and dashboard updates. A dedicated reporting and analytics module provides detailed insights into vehicle access patterns and security events, supporting informed decision-making and enhancing campus security management.

2.3 Comparison with the Existing Systems

This section provides a thorough examination and analysis of three existing systems. The features of these systems are compared against the proposed system. Table 2 presents a detailed comparison between the three existing systems and the system.

Table 2 *Comparison of the existing system and proposed system*

Criteria	License Plate Recognition System (LPR) [5]	QR Code Based System [6]	Biometric Access System [7]	Proposed System
Instant Notification Alerts for Unauthorized Access	No	No	Yes	Yes
Real-Time Monitoring Dashboard for Security Staff	Yes	No	Yes	Yes
Multi-User Role Management (Security, Staff, Student)	No	Yes	No	Yes
User-Friendly Interface for Non-Technical Users	No	Yes	No	Yes
Self-Service Vehicle and Profile Registration	No	Yes	No	Yes
Centralized Access Log and Activity Reporting	No	No	Yes	Yes
Vehicle Ownership Verification with RFID Association	No	No	No	Yes

The RFID-based vehicle access system offers the most comprehensive features compared to other methods like License Plate Recognition, QR Code systems, and Biometric Access. It is the only system that offers instant alerts for unauthorised access, real-time monitoring, multi-user role management, a simple interface, self-service registration, organised reporting, and RFID-based vehicle ownership verification. This results in a more secure, efficient, and user-friendly solution for managing campus vehicle access.

3. Methodology

The Prototyping Model, illustrated in Figure 1, is an iterative, user-centered approach to software development that emphasizes creating and refining early drafts of the system based on stakeholder feedback [8]. This model was used to develop the RFID-Based Vehicle Access and Monitoring System, ensuring it addressed real-world issues like unauthorized access and efficient vehicle tracking. The process began with the Requirements Phase to identify user needs, followed by the Quick Design Phase to define the system's structure. A functional prototype was built during the Build Prototype Phase and evaluated by stakeholders in the User Evaluation Phase. Feedback was incorporated during the Refining Prototype Phase, and the system was finalized and deployed in the Implementation and Maintain Phase for long-term use.

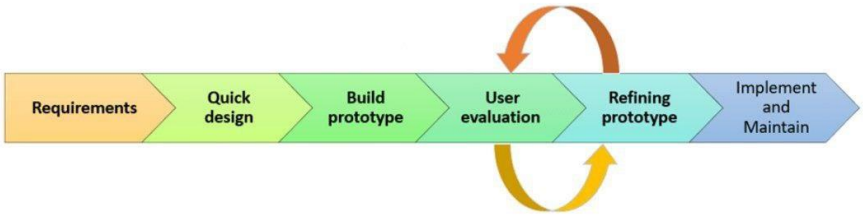


Figure 1 *Prototyping Model Flow* [8]

Table 3 shows the development workflows to build the RFID-Based Vehicle Access and Monitoring System. It is based on the Prototyping Model and includes each phase of the project, the tasks involved, the output produced, and the tools used.

Table 3 *System Development Workflow*

Phase	Activity	Work Product	Tools
Requirement	Analyze current system issues. Conduct interviews with stakeholders to identify challenges Identify functional. and non-functional requirements.	Proposal User requirement	Interview Document analysis
Quick Design	Design UML diagrams. Develop wireframes and user interface. Create a database schema.	UML diagrams Wireframe	Draw.io Visual Studio Code PhpMyAdmin
Build Prototype	Develop basic modules with functionalities. Integrate the system with the database.	Early prototype Database structure	Arduino IDE Visual Studio Code PhpMyAdmin
User Evaluation	Show the prototype to stakeholders for review. Conduct evaluation sessions. Document the feedback	User feedback Evaluation result	Feedback form Testing tools
Refining Prototype	Address issues based on feedback Enhance system performance	Refined prototype	Visual Studio Code
Implementation and Maintain	Finalize integration of all modules Verify the system is fully functioning.	Fully functional system	Visual Studio Code PhpMyAdmin

The development process began with the Requirement Phase, which involved identifying system issues and gathering user requirements through interviews and document analysis. This was followed by the Quick Design Phase, where UML diagrams, wireframes, and the database schema were created using tools like Draw.io and PhpMyAdmin. In the Build Prototype Phase, core functionalities were implemented and integrated into the database using Arduino IDE and Visual Studio Code. During the User Evaluation Phase, feedback was collected

from stakeholders to assess the system's usability and performance. The Refining Prototype Phase focused on addressing issues and enhancing the system based on the feedback received. Finally, in the Implementation and Maintain Phase, all modules were fully integrated and tested to ensure the system was operational and ready for deployment.

4. Analysis and Design

This section discussed the analysis and design that were done for the RFID-based vehicle access and monitoring system.

4.1 System Requirement Analysis

The requirement analysis phase ensures the system meets stakeholder needs and constraints, producing a systematic design [9]. Functional requirements focus on features like user registration, access control, and RFID-based vehicle identification, while non-functional requirements address system quality attributes such as performance, security, and usability. This comprehensive analysis forms the foundation for the effective design and development of the RFID-Based Vehicle Access and Monitoring System, enhancing security and operational efficiency at Universiti Tun Hussein Onn Malaysia (UTHM).

4.1.1 Use Case Diagram

Unified Model Language (UML) understandably communicates complex system designs by employing a variety of diagram types, including use cases, class diagrams, sequence diagrams, and activity diagrams. Use cases can be described with different levels of detail and may be divided into simpler use cases for better understanding. In the interaction view, a use case is carried out through the collaboration of system components [10]. Figure 2 shows the use case diagram of the proposed system.

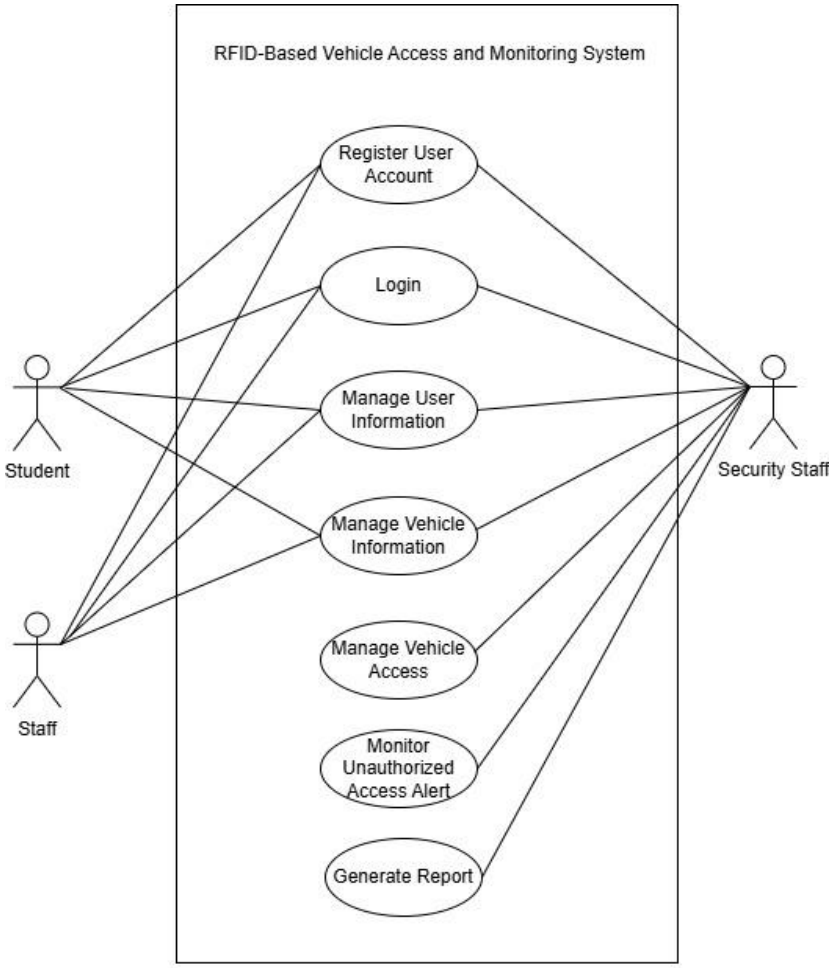


Figure 2 *Use Case Diagram*

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 1416-1435

4.1.2 Functional and Non-Functional Requirements

The system outlines seven specific functional requirements, as shown in Table 4, which illustrates the modules and functionalities of the system.

Table 4 *Functional Requirement of RFID-Based Vehicle Access and Monitoring System*

Modules	Functionalities
Register user account	• The system shall allow users to create accounts by registering with their ID number, staff or matric number, email, and password. • Registered users shall be able to log in using their credentials.
Login	• The system shall allow authorized users to log in using secure credentials (username and password). • The system shall implement role-based access, providing distinct permissions for security staff and regular users (students/staff). • The system shall display error messages for incorrect login attempts and lock the account after multiple failed attempts.
Manage User Information Module	• The system shall allow security staff to register and update user information, such as contact details, and vehicle details. • The system shall allow security staff to view and manage access logs for individual users.
Manage Vehicle Information Module	• Users shall be able to register vehicles by providing details like vehicle number, owner name, and associated RFID tag. • Security staff shall verify and approve the vehicle registration before activating RFID access.
Manage Vehicle Access Module	• The system shall verify RFID tags at entry points and grant or deny access based on database records. • The system shall log all access attempts (authorized and unauthorized) with time and RFID tag details. • The system shall notify security staff about any unauthorized access attempts.
Monitor Unauthorized Access Alert Module	• The system shall detect and trigger alerts for unregistered or unauthorized vehicles attempting entry. • Alerts shall be sent to the security dashboard in real-time for further action.
Generate Report Module	• The system shall generate reports for access history, including details like date, time, vehicle number, and user information. • The system shall allow security staff to filter reports by date, vehicle type, or user category (staff or students).

The RFID-Based Vehicle Access and Monitoring System includes seven main modules with functional requirements. These modules handle user registration and login, manage user and vehicle information, control vehicle access, monitor unauthorized access, and generate reports. Each module is designed to enhance system security, ensure proper data management, and provide real-time alerts and access control. Security staff are given specific access rights, and RFID tags are used to log and verify vehicle entries accurately.

Table 5 shows a detail description of the non-functional requirement of the system.

Table 5 *Non-Functional Requirement of RFID-Based Vehicle Access and Monitoring System*

Requirement	Description
Performance	The system must process RFID tag scans and grant or deny access within 2 seconds.
Operational	The system shall operate 24/7 with minimal downtime.
Security	The system shall encrypt RFID communications and stored data.
Usability	The interface must be user-friendly so that security staff can navigate the system easily.

The system's non-functional requirements focus on performance, reliability, security, and usability. It is designed to process RFID scans quickly within 2 seconds and operate continuously with minimal downtime. Strong security features are implemented to protect user data, and the interface is made user-friendly so that even non-technical security staff can use it easily.

4.1.3 Domain Class Diagram

The class diagram illustrated in Figure 3, is the conceptual model in database modeling [7]. It includes PR_General, PR_User, VE_Vehicle, VE_VehicleData, VE_AccessLog, VE_AccessNoti, VE_OpenAccess, KM_StatusApplied, RF_Tag, KM_TagStatus, and KM_AccessStatus.

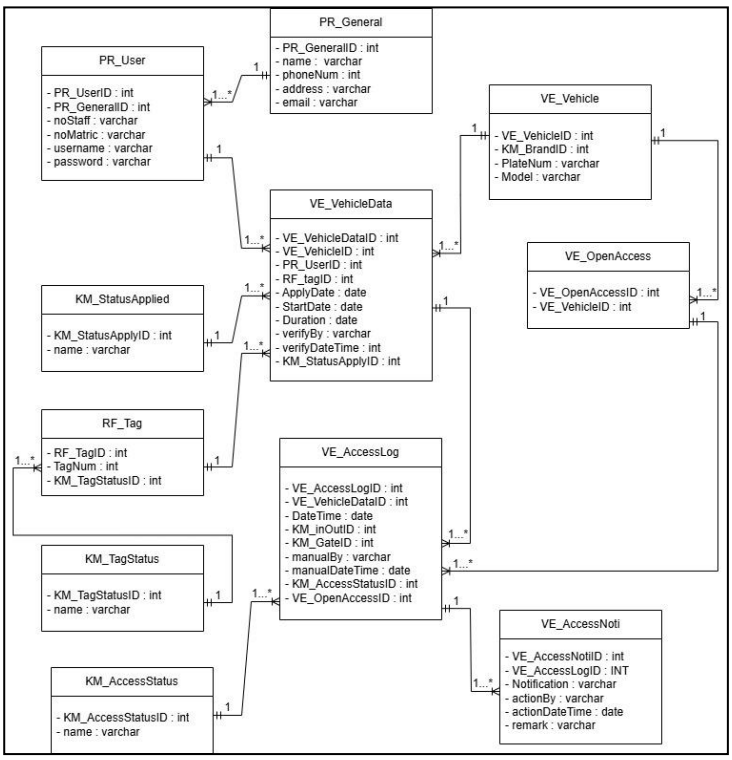


Figure 3 *Domain Class Diagram*

4.2 Design

4.1.4 System Architecture

The RFID-Based Vehicle Access and Monitoring System applies a client-server architecture, as shown in Figure 4. Users, including students, staff, and security staff, interact with a centralised MySQL server through user interfaces. Each role can access specific modules, such as vehicle information management, access control, and reporting. The system provides secure, role-based access while maintaining efficient communication between frontend interfaces and backend databases.

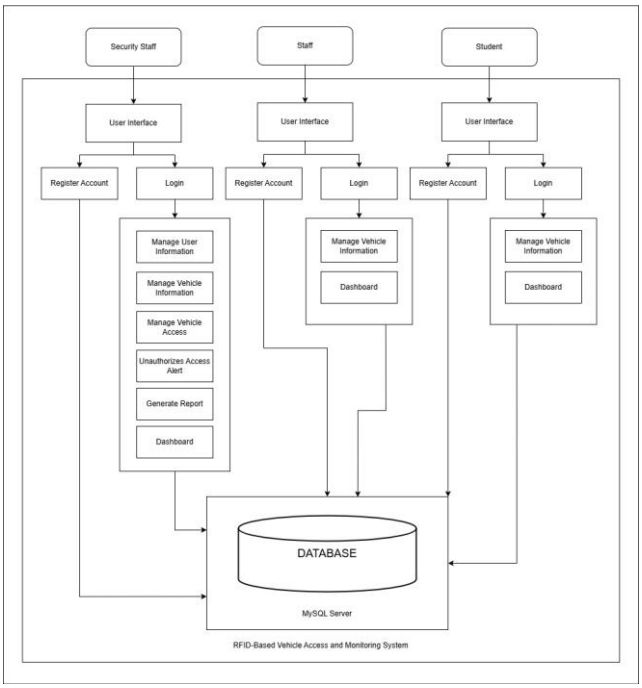


Figure 4 *System Architecture for RFID-Based Vehicle Access and Monitoring System*

4.1.5 Hardware and Software Requirement Analysis

Hardware and software requirements are shown in Tables 6 and 7.

Table 6 *Hardware Requirements*

Requirement	Description
Arduino Uno R3	Serves as the main microcontroller for processing input/output signals.
RFID card reader writer module	Reads the RFID tag ID from vehicle tags to verify access credentials.
Mini servo motor sg-90	Operates the gate arm mechanism by rotating based on access authorization.
Traffic lights module	Simulates traffic signals using Red, Green and Orange LEDs to indicate access status
40 pin male to male jumper wire	Facilitates electrical connections between hardware components on the breadboard
Hard jumper wire 1 meter	Provides power supply across longer distances within the circuit setup.
LCD	Outputs messages such as tag ID status, access approval, or denial.

Table 7 *Software Requirements*

Requirement	Description
Visual Studio Code	Used as the main code editor for writing and managing front-end and PHP scripts.
Arduino IDE	Used to write, compile, and upload code to the Arduino Uno microcontroller.
PhpMyAdmin	Web-based tool for managing the MySQL database, including tables and queries.
XAMPP	Provides a local server environment for running PHP scripts and MySQL database.

The system requires specific hardware and software components to function effectively. The hardware includes devices like the Arduino Uno R3 as the main controller, an RFID reader for scanning tags, a servo motor for gate control, and supporting components such as traffic lights, jumper wires, and an LCD for displaying messages, as shown in Table 6. On the software side, development and system operation rely on tools such as

Visual Studio Code, Arduino IDE, PhpMyAdmin, and XAMPP to support coding, database management, and server deployment, as shown in Table 7.

4.1.6 User Interface Design

The user interfaces of the system were designed using Visual Studio Code. Figure 5, Figure 6, Figure 7 and Figure 8 display the essential interface designs of the proposed system. Additional interface designs can be found in Appendix C.

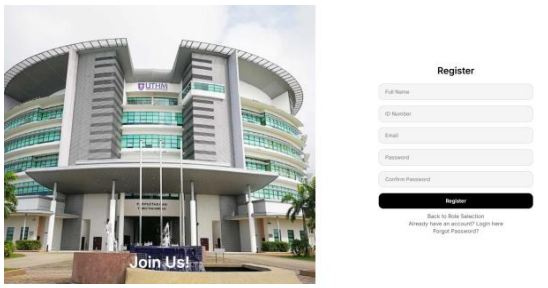


Figure 5 *Register Interface*

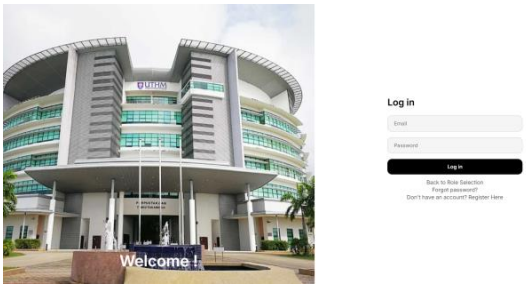


Figure 6 *Login Interface*

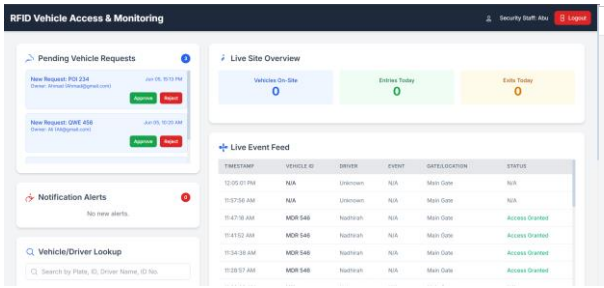


Figure 7 *Dashboard for Security Staff*

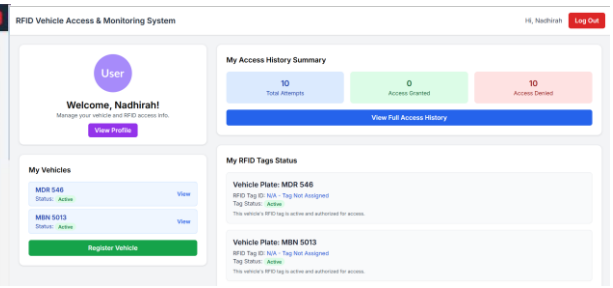


Figure 8 *Dashboard for User (Staff and Student)*

4.1.7 Database

The database schema obtained from the class diagram is listed as follows, highlighting the structure of each table and its attributes:

I. PR_User (PR_UserID, PR_GeneralID, NumID, username, password)
II. PR_General (PR_GeneralID, name, phoneNum, address, email)
III. VE_Vehicle (VE_VehicleID, KM_BrandID, PlateNum, Model, Color)
IV. VE_VehicleData (VE_VehicleDataID, VE_VehicleID, PR_UserID, RF_tagID, ApplyDate, StartDate, Duration, verifyBy, verifyDateTime, KM_StatusApplyID)
V. VE_AccessLog (VE_AccessLogID, VE_VehicleDataID, DateTime, KM_inOutID, KM_GateID, manualBy, manualDateTime, KM_AccessStatusID, VE_OpenAccessID)
VI. VE_OpenAccess (VE_OpenAccessID, VE_VehicleID)
VII. VE_AccessNoti (VE_AccessNotiID, VE_AccessLogID, Notification, actionBy, actionDateTime, remark)
VIII. RF_Tag (RF_TagID, TagNum, KM_TagStatusID)
IX. KM_TagStatus (KM_TagStatusID, name)
X. KM_StatusApplied (KM_StatusApplyID, name)
XI. KM_AccessStatus (KM_AccessStatusID, name)

The database schema was designed in advance to ensure the identification of essential data elements and the relationships between them.

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 1416-1435

5. Result and Discussion

This section presents the implementation of the system modules, detailing their functionalities and integration. It also provides a discussion of the testing results.

5.1 Implementation

The Register User Account module is developed using PHP and MySQL. The interface is designed using HTML and CSS, while the backend logic is implemented with PHP. This module allows a new user to create an account in the system by providing personal details such as full name, ID Number, email address, and password. These details are then securely stored in the MySQL database. The registered credentials, particularly the email and password, are essential for future logins. The system includes basic validation to ensure that all fields are completed correctly and that duplicate email addresses are not accepted. Upon successful registration, the user receives confirmation and is redirected to the login page. The Register User Account Interface is illustrated in Figure 9, and the corresponding Code Segment for Register User Account is shown in Figure 10.

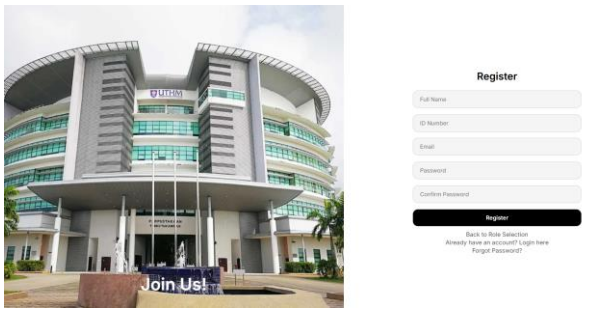


Figure 9 *Register User Account Interface*

```php
// Validate password
if ($password !== $confirm_password) {
    $error = "Passwords do not match.";
} elseif (!preg_match('/^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[\W_]).{8,}$/', $password)) {
    $error = "Password must be at least 8 characters and include uppercase, lowercase, number, and special character.";
} else {
    // Check for duplicate email or ID number
    $stmt = $conn->prepare("SELECT * FROM users WHERE email = ? OR id_number = ?");
    $stmt->bind_param("ss", $email, $id_number);
    $stmt->execute();
    $result = $stmt->get_result();

    if ($result->num_rows > 0) {
        $error = "Email or ID number already registered.";
    } else {
        // Insert new user
        $password_hash = password_hash($password, PASSWORD_DEFAULT);
        $stmt = $conn->prepare("INSERT INTO users (username, id_number, email, password_hash, role) VALUES (?, ?, ?, ?, ?)");
        $stmt->bind_param("sssss", $username, $id_number, $email, $password_hash, $role);

        if ($stmt->execute()) {
            $success = "Registration successful! You can now <a href='login.php'>login</a>.";
        } else {
            $error = "Registration failed. Please try again.";
        }
    }
    $stmt->close();
}
```

Figure 10 *Register User Account Code Segment*

This Login module enables registered users to securely access the system by entering their email address and password. The credentials entered are validated against the user information stored in the MySQL database. Upon submission, the system checks whether the provided email and password match any existing records. If the login is successful, the user is granted access to the system dashboard based on their assigned role. If the credentials are incorrect, an error message is displayed, prompting the user to re-enter the correct details.

Security measures such as password hashing and session management are used to protect user data and prevent unauthorised access. Figure 10 shows the Login Interface, while Figure 11 shows the corresponding Login Code Segment.

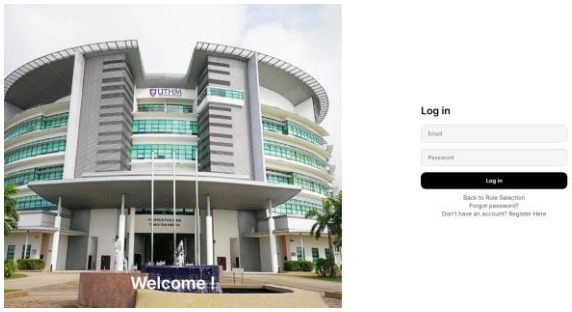


Figure 10 *Login Interface*

```php
try {
    $stmt = $conn->prepare("SELECT id, username, role, password_hash FROM users WHERE email = ?");
    $stmt->bind_param("s", $email);
    $stmt->execute();
    $result = $stmt->get_result();

    if ($result->num_rows === 1) {
        $user = $result->fetch_assoc();

        if (password_verify($password, $user['password_hash'])) {
            // Store user data in session
            $_SESSION['user_id'] = $user['id'];
            $_SESSION['username'] = $user['username'];
            $_SESSION['role'] = $user['role'];

            // Redirect based on role
            switch ($user['role']) {
                case 'staff':
                    header("Location: DashboardStaff.php");
                    exit;
                case 'user':
                    header("Location: DashboardUser.php");
                    exit;
                default:
                    $error = "Unknown role. Please contact the administrator.";
            }
        } else {
            $error = "Incorrect password. Please try again.";
        }
    } else {
        $error = "No account found with that email.";
    }
} catch (Exception $e) {
    $error = "An error occurred: " . $e->getMessage();
}
```

Figure 11 *Login Code Segment*

The Manage User Information module is designed to allow users and security staff to view and update user-related data based on their respective roles. For security staff, this interface provides extended access to view and update the information of all registered users in the system, including their full name, email address, phone number, gender, and assigned roles (e.g., student, staff). This facilitates administrative control and ensures that user records remain up-to-date. The interface for security staff is shown in Figure 12.

For staff and students, the interface is limited to personal information management. Users can view and edit only their own details such as name, phone number, and email. This ensures data privacy and role-based access control. The interface for staff and students is shown in Figure 13.

All changes made are validated before being updated in the database. The corresponding Code Segment for the Manage User Information Module is presented in Figure 14.

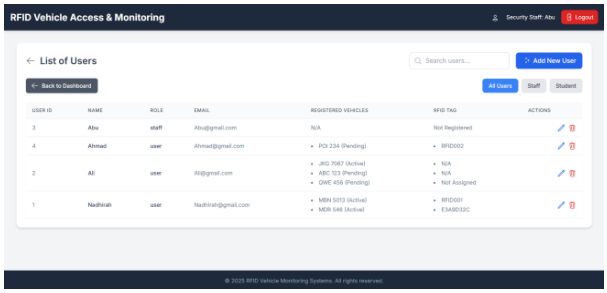


Figure 12 *Manage User Information Interface (security staff)*

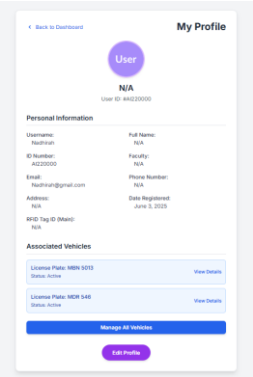


Figure 13 *Manage User Information Interface (Staff & Student)*

```php
if ($result_users) {
    while ($user_row = $result_users->fetch_assoc()) {
        $user_id = $user_row['id'];
        $user_data = [
            'userId' => $user_row['id'],
            'name' => $user_row['username'],
            'role' => $user_row['role'],
            'email' => $user_row['email'],
            'registeredVehicles' => [], // To store details of vehicles for this user
        ];

        $stmt_vehicles = $conn->prepare("SELECT plate_number, tag_id, status FROM vehicles WHERE user_id = ?");
        if (!$stmt_vehicles) {
            error_log("Failed to prepare vehicle statement: " . $conn->error);
            throw new Exception("Failed to prepare vehicle statement.");
        }
        $stmt_vehicles->bind_param("i", $user_id);
        $stmt_vehicles->execute();
        $result_vehicles = $stmt_vehicles->get_result();

        while ($vehicle_row = $result_vehicles->fetch_assoc()) {
            $user_data['registeredVehicles'][] = [
                'plate_number' => $vehicle_row['plate_number'],
                'rfid_tag' => $vehicle_row['tag_id'] ?? 'N/A',
                'status' => $vehicle_row['status']
            ];
        }
        $stmt_vehicles->close();

        $users_data[] = $user_data;
    }
} else {
    $error_message = "Error fetching users: " . $conn->error;
}
```

Figure 14 *Manage User Information Code Segment*

The Manage Vehicle Information module allows users and security staff to add, view, and update vehicle-related details in the system. For security staff, the interface provides full access to all registered vehicles in the system. Security staff can view, update, and manage the vehicle details of any user, including vehicle type, model, license plate number, and the owner's name. This functionality helps in maintaining a comprehensive vehicle database for monitoring and access control. The interface for security staff is shown in Figure 15.

For staff and students, the interface is limited to their own vehicle records. They can register a new vehicle, view existing details, or make updates to their personal vehicle information when necessary. This access is restricted to maintain privacy and role-based system integrity. The interface for staff and students is illustrated in Figure 16.

Each action within this module, such as adding or updating vehicle information, is validated and stored securely in the MySQL database. The Code Segment for the Manage Vehicle Information Module is shown in Figure 17.

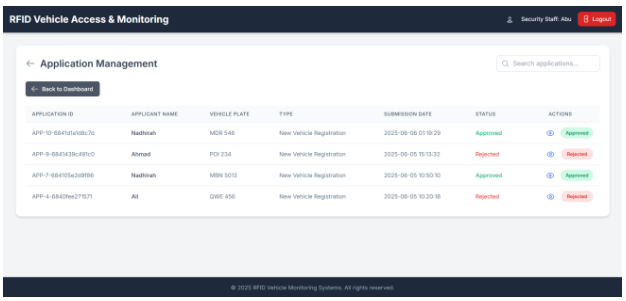


Figure 15 *Manage Vehicle Information Interface (Security staff)*

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 1416-1435

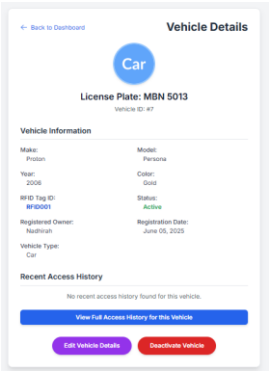
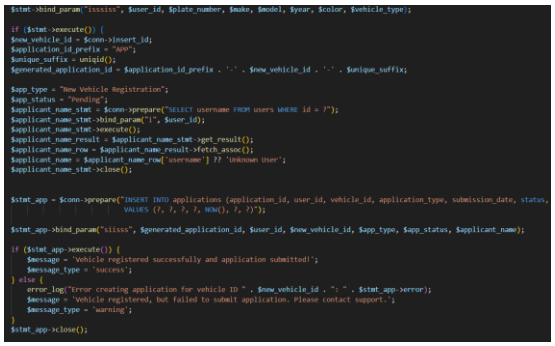


Figure 16 *Manage Vehicle Information Interface (Staff & Student)*



```
$stmt->bind_param("ssssiss", $user_id, $plate_number, $make, $model, $year, $color, $vehicle_type);

if ($stmt->execute()) {
$new_vehicle_id = $conn->insert_id;
$application_id_prefix = "APP";
$unique_suffix = uniqid();
$generated_application_id = $application_id_prefix . '-' . $new_vehicle_id . '-' . $unique_suffix;

$app_type = "New Vehicle Registration";
$app_status = "Pending";
$applicant_name_stmt = $conn->prepare("SELECT username FROM users WHERE id = ?");
$applicant_name_stmt->bind_param("i", $user_id);
$applicant_name_stmt->execute();
$applicant_name_result = $applicant_name_stmt->get_result();
$applicant_name_row = $applicant_name_result->fetch_assoc();
$applicant_name = $applicant_name_row['username'] ?? 'Unknown User';
$applicant_name_stmt->close();


$stmt_app = $conn->prepare("INSERT INTO applications (application_id, user_id, vehicle_id, application_type, submission_date, status,
                            VALUES (?, ?, ?, ?, NOW(), ?, ?)");

$stmt_app->bind_param("siissss", $generated_application_id, $user_id, $new_vehicle_id, $app_type, $app_status, $applicant_name);

if ($stmt_app->execute()) {
    $message = 'Vehicle registered successfully and application submitted!';
    $message_type = 'success';
} else {
    error_log("Error creating application for vehicle ID " . $new_vehicle_id . ": " . $stmt_app->error);
    $message = 'Vehicle registered, but failed to submit application. Please contact support.';
    $message_type = 'warning';
}
$stmt_app->close();
```

Figure 17 *Manage Vehicle Code Segment*

The Manage Vehicle Access module is a core component of the system that enables security staff to control and monitor vehicle entry permissions. Through this module, security staff can review registered vehicles and grant or deny access permissions based on various criteria such as user role, vehicle status, or location. The interface allows for easy updating of access status (e.g., "Allowed" or "Denied") for each vehicle, ensuring only authorized vehicles are permitted to enter the campus.

Additionally, this module supports real-time updates to vehicle access rights and maintains a log of changes for security auditing purposes. The interface for managing vehicle access is shown in Figure 18, while the Code Segment for the Manage Vehicle Access Module is presented in Figure 19.

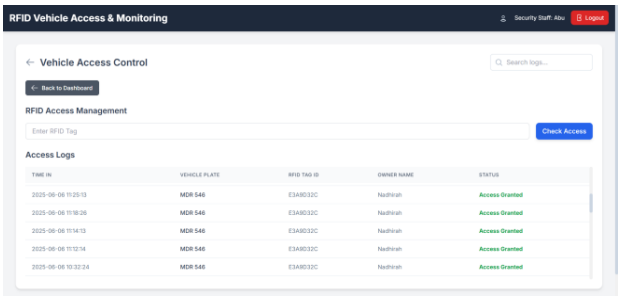


Figure 18 *Manage Vehicle Access Interface*

```
if ($_SERVER["REQUEST_METHOD"] == "POST" && isset($_POST['rfid_tag'])) {
    $input_rfid_tag = $conn->real_escape_string($_POST['rfid_tag']);
    $access_time = date('Y-m-d H:i:s');
    $location = 'Main Gate';

    $owner_name = 'Unknown';
    $vehicle_db_id = NULL;
    $plate_number_for_log = 'N/A';
    $status = 'Access Denied';

    $check_sql = "SELECT v.id AS vehicle_id, v.plate_number, v.status AS vehicle_status, u.username AS owner_name
                  FROM vehicles v
                  LEFT JOIN users u ON v.user_id = u.id
                  WHERE v.tag_id = ? LIMIT 1";

    $stmt_check = $conn->prepare($check_sql);
    if ($stmt_check) {
        $stmt_check->bind_param("s", $input_rfid_tag);
        $stmt_check->execute();
        $result_check = $stmt_check->get_result();

        if ($result_check && $result_check->num_rows > 0) {
            $vehicle_row = $result_check->fetch_assoc();
            $owner_name = htmlspecialchars($vehicle_row['owner_name'] ?? 'N/A');
            $vehicle_db_id = $vehicle_row['vehicle_id'];
            $plate_number_for_log = htmlspecialchars($vehicle_row['plate_number'] ?? 'N/A');
            $vehicle_status = $vehicle_row['vehicle_status'];

            if ($vehicle_status === 'Active') {
                $status = "Access Granted";
            } else {
                $status = "Access Denied - Vehicle " . $vehicle_status;
            }
        }
        $stmt_check->close();
```

Figure 19 *Manage Vehicle Access Code Segment*

The Monitor Unauthorized Access Alert module is designed to enhance system security by detecting and responding to unauthorized vehicle access attempts. When a vehicle without valid access credentials attempts to pass through the RFID-based checkpoint, the system automatically identifies the violation and triggers an alert. This alert includes key information such as the tag ID, timestamp, location, and vehicle owner's name. All unauthorized attempts are recorded in the database for monitoring and auditing purposes.

Security staff can view these alerts in real time through a dedicated interface that provides quick access to critical data. This enables timely action such as verifying the incident or updating access permissions. The Monitor Unauthorized Access Alert Interface is illustrated in Figure 20, and the corresponding Code Segment is shown in Figure 21.

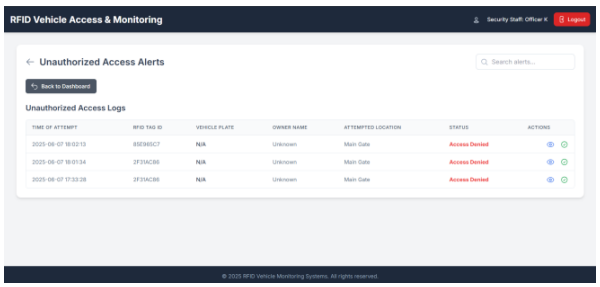


Figure 20 *Monitor Unauthorized Access Alert Interface*

```
if ($logId) {
    $update_sql = "UPDATE access_log SET status = 'Resolved' WHERE id = ?";
    $stmt = $conn->prepare($update_sql);
    if ($stmt) {
        $stmt->bind_param("i", $logId); // Assuming 'id' is an integer
        $stmt->execute();
        if ($stmt->affected_rows > 0) {
            error_log("Alert ID " . $logId . " marked as resolved in DB.");
            header('Content-Type: application/json');
            echo json_encode(['success' => true, 'message' => 'Alert marked as resolved.']);
            exit;
        } else {
            error_log("Failed to mark Alert ID " . $logId . " as resolved. No rows affected.");
            header('Content-Type: application/json');
            echo json_encode(['success' => false, 'message' => 'Failed to mark alert as resolved: No changes or record not found.']);
            exit;
        }
        $stmt->close();
    } else {
        error_log("Failed to prepare update statement: " . $conn->error);
        header('Content-Type: application/json');
        echo json_encode(['success' => false, 'message' => 'Database error during update preparation.']);
        exit;
    }
} else {
    error_log("Log ID not provided for marking as resolved.");
    header('Content-Type: application/json');
    echo json_encode(['success' => false, 'message' => 'Log ID is missing for resolution.']);
    exit;
}
```

Figure 21 *Monitor Unauthorized Access Alert Code Segment*

The Generate Report module provides authorized users, particularly security staff, with the ability to generate and download comprehensive reports based on vehicle access data. This module allows filtering of data based on various parameters such as date range, access status (authorized or unauthorized), location, user type, and vehicle details. The generated reports are displayed in a tabular format and can be exported in PDF or CSV format for documentation, analysis, or audit purposes. The system ensures that reports are accurate and up to date, supporting better decision-making and improving the overall security management process. The Generate Report Interface is shown in Figure 22, while the Code Segment for the Generate Report Module is presented in Figure 23.

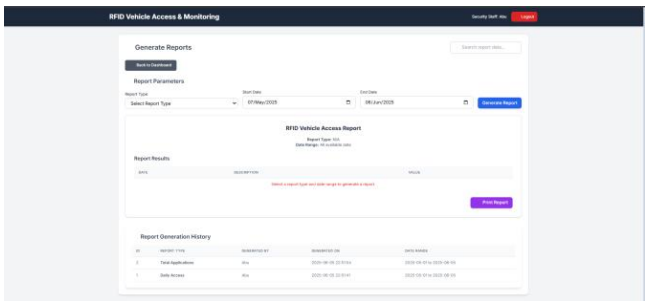


Figure 22 *Generate Report Interface*

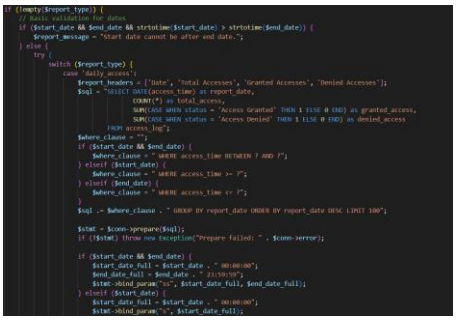


Figure 23 *Generate Report Code Segment*

5.2 Testing

The RFID-based vehicle access and monitoring system is tested to ensure it meets all the required specifications. There are two types of testing: functional requirements testing and user acceptance testing.

The functional testing evaluates each module to ensure the system functions as expected. Each test case represents a specific system function, such as user registration, RFID scanning, or unauthorised access alerts. Table 8 summarises the test results, displaying the number of test cases executed and how many passed successfully.

Table 8 *Overall Test Case Result*

Test Case ID	Total Test Cases	Total Passed
TEST_100	5	5
TEST_200	6	6
TEST_300	6	6
TEST_400	6	6
TEST_500	6	6
TEST_600	8	8
TEST_700	5	5
	42	42

User acceptance testing was conducted with a group of ten participants, including staff, students, and security staff. The users were asked to rate the system on a scale of 1 to 5, with 1 being very dissatisfied and 5 being very satisfied. They were instructed to evaluate usability, visual design, feature clarity, and performance. The purpose of this test is to determine the ease of use and overall satisfaction of the users while interacting with the RFID vehicle access and monitoring system. The feedback gathered provides insight into real-world usability and is summarized through descriptive statistics in Table 9, offering a clearer view of overall user satisfaction and system effectiveness, further illustrated in Figure 24 through the average score chart.

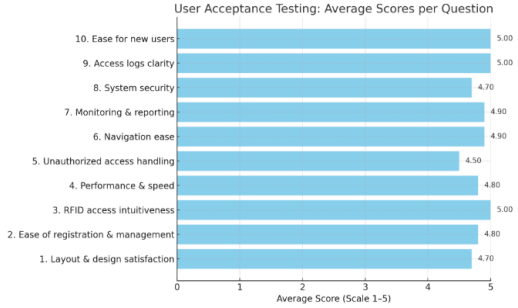


Figure 24 *Summary of user acceptance testing average score*

Table 9 *Summary of descriptive statistics for RFID-Based Vehicle Access and Monitoring System*

No.	Question	Mean	Median	Mode	Standard Deviation
1.	How satisfied are you with the overall layout and design of the system interface?	4.7	5.0	5	0.46
2.	How easy is it to register and manage user and vehicle information in the system?	4.8	5.0	5	0.40
3.	How intuitive is the RFID vehicle access process (e.g., scanning RFID tag, gate operation)?	5.0	5.0	5	0.00
4.	How satisfied are you with the system's performance and speed during use?	4.8	5.0	5	0.40
5.	How well does the system alert and handle unauthorized vehicle access?	4.5	5.0	5	0.67
6.	How easy is it to navigate between modules (e.g., dashboard, user info, vehicle logs)?	4.9	5.0	5	0.30
7.	How satisfied are you with the real-time monitoring and reporting features?	4.9	5.0	5	0.30
8.	How secure do you feel the system is in preventing unauthorized vehicle access?	4.7	5.0	5	0.46
9.	How satisfied are you with the visual presentation and clarity of vehicle access logs?	5.0	5.0	5	0.00
10.	How easy is it to understand and use the system's main features as a new user?	5.0	5.0	5	0.00

All of the user responses were highly positive, with over 90% of ratings being either 4 or 5. The system received consistently high scores across all features. Users found it intuitive, simple to use, and satisfactory in terms of design, performance, and security. 100% of respondents gave perfect scores (5/5) for critical functions such as RFID access, module navigation, and system understanding as a new user. Even the few instances of slightly lower ratings—mainly on security alerts—still scored a 3 or 4, indicating no negative feedback. Overall, user acceptance testing shows that the system was very well-received, with an average rating of 4.8 out of 5. User feedback indicates that the system is highly successful. Most users were pleased with its design, ease of use for core functions such as registration, and clear, intuitive processes. Key features like navigation, logging, and performance received 90%–100% scores of 5, highlighting strong user satisfaction. The only minor suggestion for improvement was one user's slightly lower rating for security alerts, but overall, the system is regarded as highly effective and user-friendly.

6. Conclusion

The development of the RFID-Based Vehicle Access and Monitoring System for Universiti Tun Hussein Onn Malaysia (UTHM) addresses critical challenges associated with the university's manual vehicle access processes, including inefficiencies, human errors, and security risks. By applying RFID technology and a web-based platform, the system improves vehicle access management and introduces modules for user authentication, vehicle registration, real-time access monitoring, and reporting. These characteristics ensure a convenient and secure campus vehicle access system and are suitable for the roles of staff, students, and security staff. The iterative development approach, guided by stakeholder feedback and employing the prototyping model, ensures that the system aligns with UTHM's security needs while enhancing usability and operational efficiency. Upon implementation, the RFID-Based Vehicle Access and Monitoring System is expected to streamline vehicle entry processes, improve data accuracy, reduce manual errors, and enhance campus security management. Finally, this system contributes to creating a safer, more efficient, and technology-driven environment for the UTHM community.

Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support.

Conflict of Interest

Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution

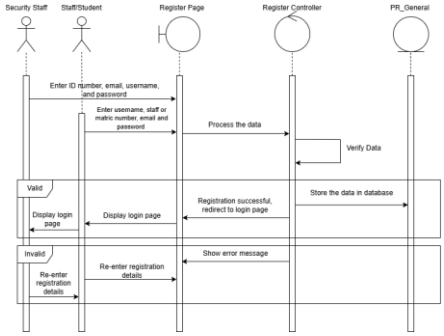
The authors confirm contribution to the paper as follows: ***study conception and design:*** *Nur Nadhirah Binti Masri, Ruhaya Binti Ab. Aziz;* ***data collection:*** *Nur Nadhirah Binti Masri, Ruhaya Binti Ab. Aziz;* ***analysis and interpretation of results:*** *Nur Nadhirah Binti Masri, Ruhaya Binti Ab. Aziz;* ***draft manuscript preparation:*** *Nur Nadhirah Binti Masri, Ruhaya Binti Ab. Aziz. All authors reviewed the results and approved the final version of the manuscript.*

References

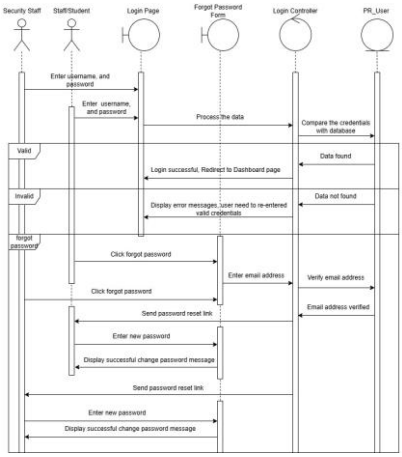
[1] R. H. Saeed, F. N. Qassabbashi, L. M. Saeed, and F. Mahmood, "Vehicle Accessibility Using RFID Technology," *Przegląd Elektrotechniczny*, vol. 99, no. 7, pp. 65-68, 2023.
[2] Priyanka, "The future of RFID in access management," *International Journal of Technology*, vol. 9, no. 2, pp. 89-94, 2017.
[3] E. Hassania Rouan and A. Boumezzough, "RFID Based Security and Automatic Parking Access Control System," in *Lecture Notes in Business Information Processing*, Springer Nature, May 2021, pp. 434–443. doi: 10.1007/978-3-030-76508-8_32
[4] FRESH USA, Inc., "RFID vehicle access control systems," *FRESH222*, Dec. 18, 2024. [Online]. Available: https://www.fresh222.com/rfid-vehicle-access-control-systems/
[5] M. A. M. B. Kamaruzaman and N. R. M. Nasir, "PARKEY: Ticket-less parking system using license plate recognition approach," *Journal of Physics: Conference Series*, vol. 1860, no. 1, p. 012006, 2021. https://doi.org/10.1088/1742-6596/1860/1/012006researchgate.net+5researchgate.net+5colab.ws+5
[6] N. Benjamin and V. Devi, "New QR code system running smoothly at JB checkpoint," *The Star*, Jun. 1, 2024. [Online]. Available: https://www.thestar.com.my/news/nation/2024/06/01/new-qr-code-system-running-smoothly-at-jb-checkpoint
[7] J. Shaw, "Biometrics rolling towards relevance for automakers and drivers," *Biometric Update*, Feb. 2025. [Online]. Available: https://www.biometricupdate.com/202502/biometrics-rolling-towards-relevance-for-automakers-and-drivers
[8] L. Bennet, "Prototyping Model in Software Engineering: Methodology, Process, Approach," Guru99.com, Aug. 13, 2024. https://www.guru99.com/software-engineering-prototyping-model.html
[9] P. A. Laplante and M. Kassab, *Requirements Engineering for Software and Systems*. Boca Raton, FL, USA: Auerbach Publications, 2022.
[10] J. Rumbaugh, I. Jacobson, and G. Booch, "The Unified Modeling Language Reference Manual," 2021.

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 1416-1435

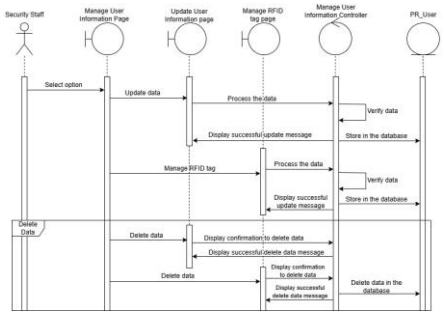
Appendix A: Sequence Diagram



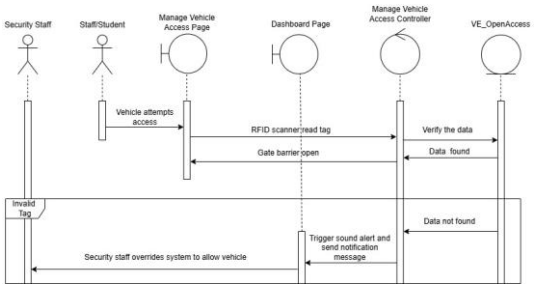
Sequence Diagram of Register User Account Module



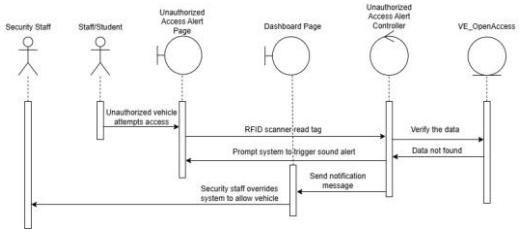
Sequence Diagram of Login Module



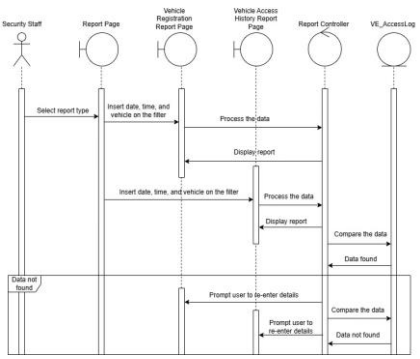
Sequence Diagram of Manage User Information Module



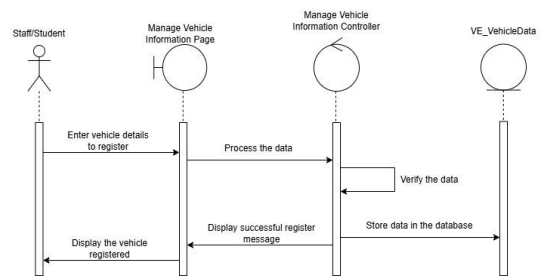
Sequence Diagram of Manage Vehicle Access Module



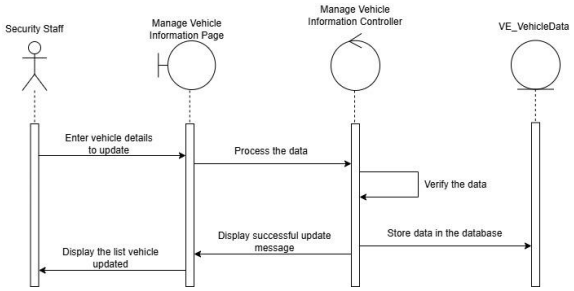
Sequence Diagram of Monitor Unauthorized Access Alert Module



Sequence Diagram of Generate Report Module

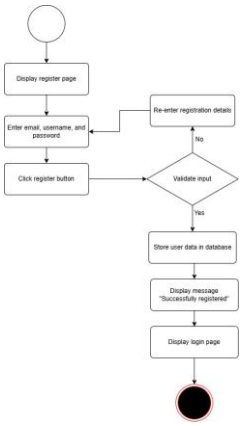


Sequence Diagram of Manage Vehicle Information Module (Staff & Student)

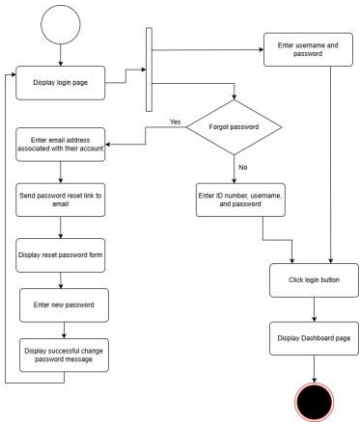


Sequence Diagram of Manage Vehicle Information Module (Security Staff)

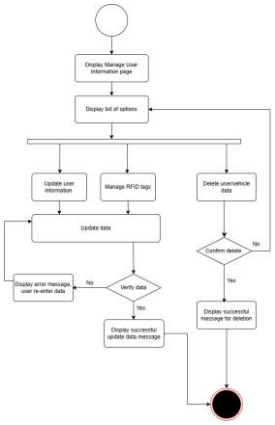
Appendix B: Activity Diagram



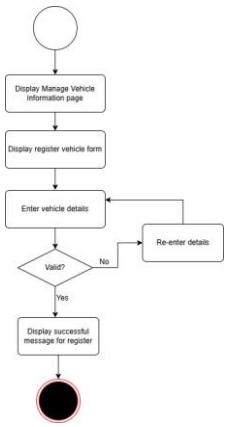
Activity Diagram of Register User Account Module



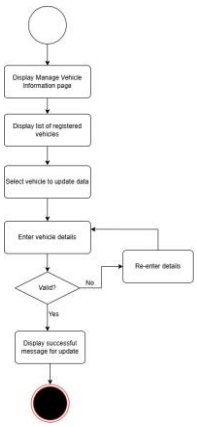
Activity Diagram of Login Module



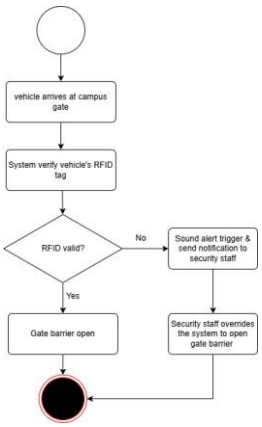
Activity Diagram of Manage User Information Module



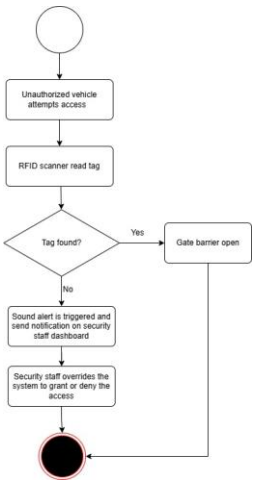
Activity Diagram of Manage Vehicle Information Module (Staff & Student)



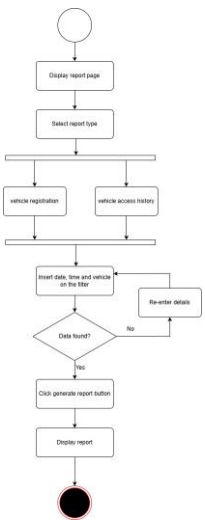
Activity Diagram of Manage Vehicle Information Module (Security Staff)



Activity Diagram of Manage Vehicle Access Module



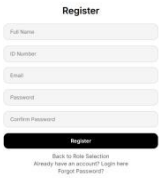
Activity Diagram of Monitor Unauthorized Access Alert Module



Activity Diagram of Generate Report Module

Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 1416-1435

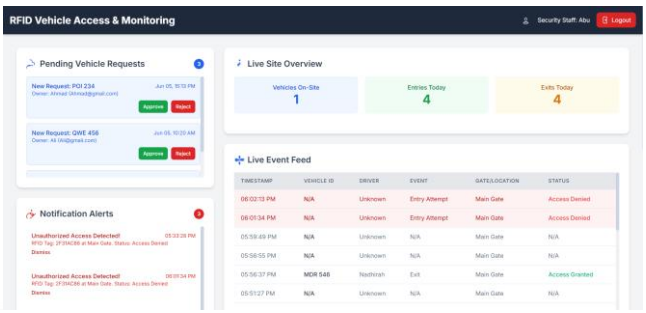
Appendix C: User Interface Design



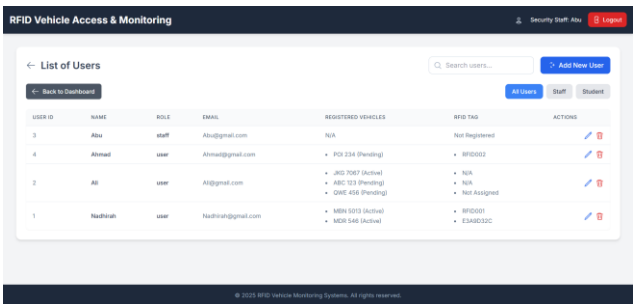
Register Interface

Login Interface

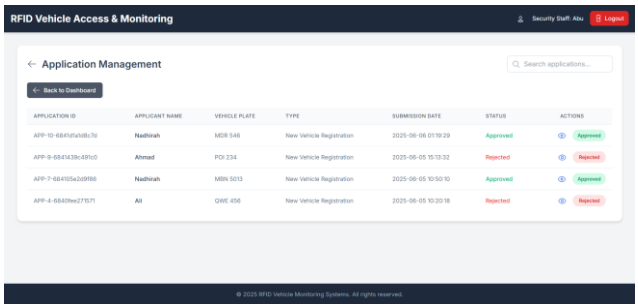
Forgot Password Interface



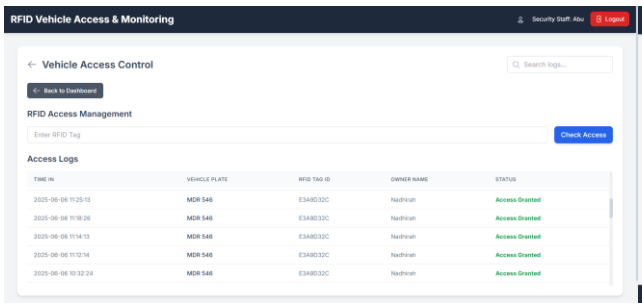
Security Staff Dashboard Interface



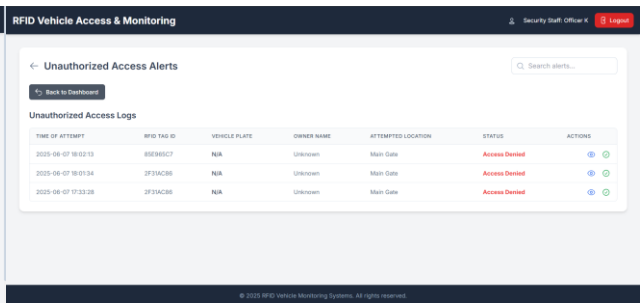
Manage User Information Interface (Security staff)



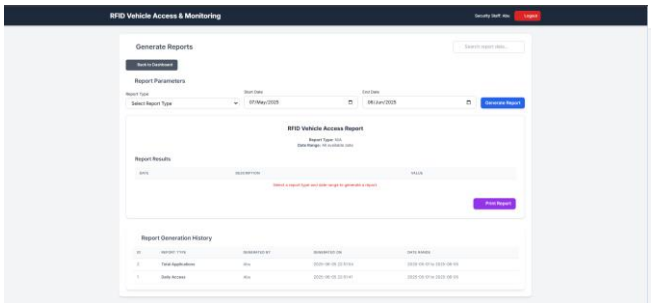
Manage Vehicle Information Interface (security staff)



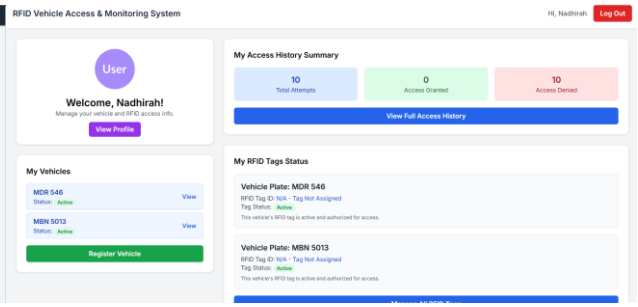
Manage Vehicle Access Interface



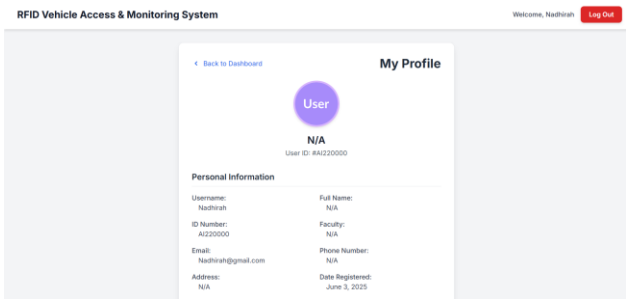
Monitor Unauthorized Access Alert Interface



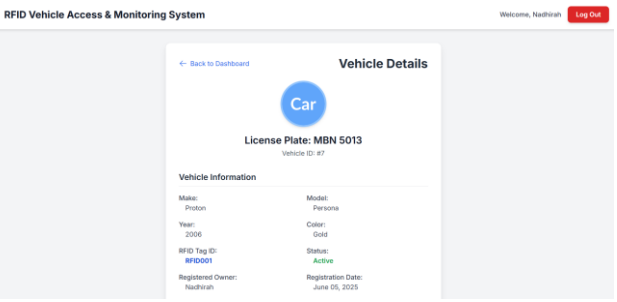
Generate Report Interface



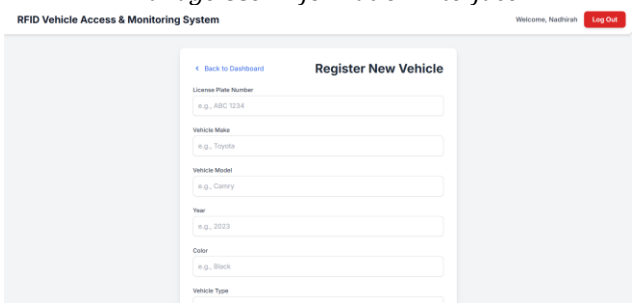
User(Staff & Student) Dashboard Interface



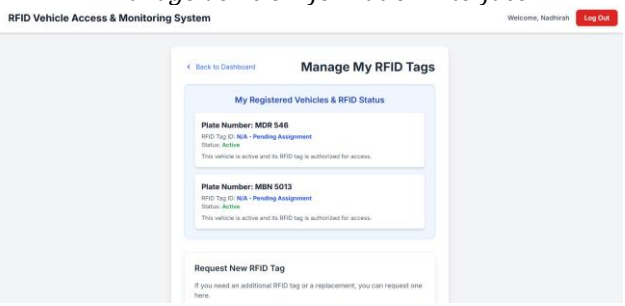
Manage User Information Interface



Manage Vehicle Information Interface



Register Vehicle Interface

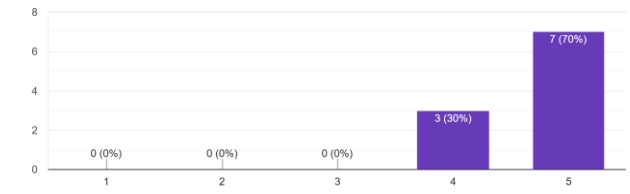


Manage RFID Tags Interface

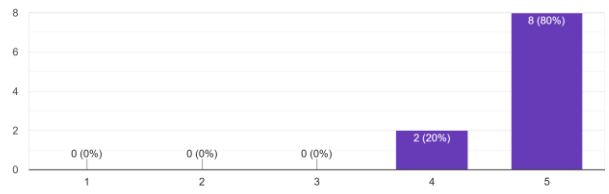
Applied Information Technology and Computer Science Vol. 6 No. 2 (2025) p. 1416-1435

Appendix D: Google Form Feedback Respondents

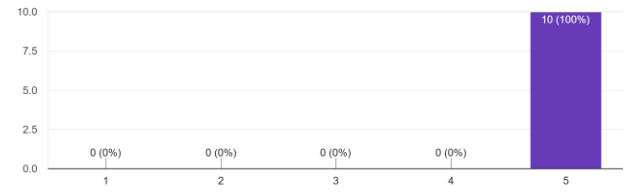
1. How satisfied are you with the overall layout and design of the system interface?
10 responses



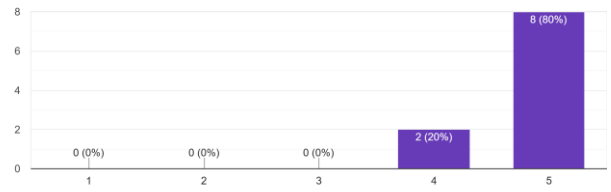
2. How easy is it to register and manage user and vehicle information in the system?
10 responses



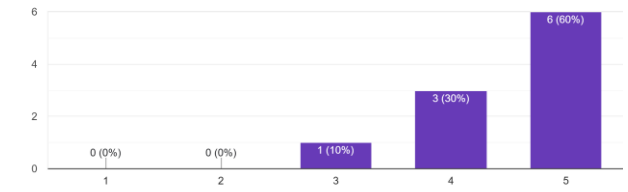
3. How intuitive is the RFID vehicle access process (e.g., scanning RFID tag, gate operation)?
10 responses



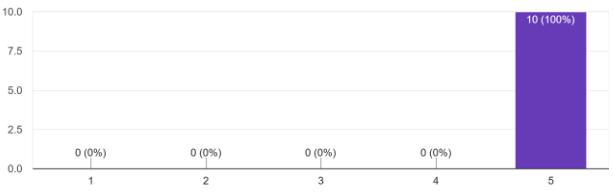
4. How satisfied are you with the system's performance and speed during use?
10 responses



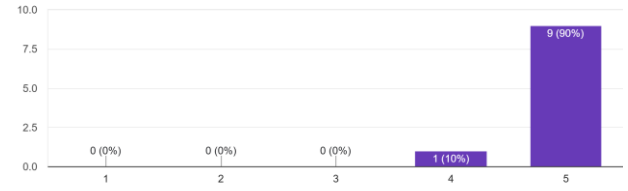
5. How well does the system alert and handle unauthorized vehicle access?
10 responses



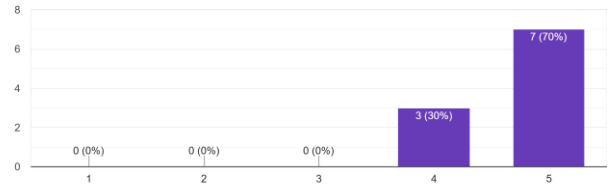
6. How easy is it to navigate between modules (e.g., dashboard, user info, vehicle logs)?
10 responses



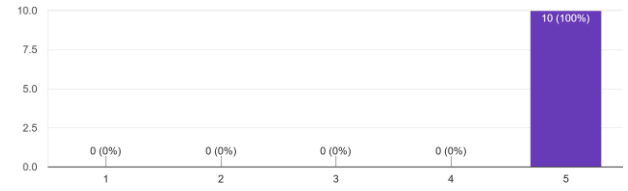
7. How satisfied are you with the real-time monitoring and reporting features?
10 responses



8. How secure do you feel the system is in preventing unauthorized vehicle access?
10 responses



9. How satisfied are you with the visual presentation and clarity of vehicle access logs?
10 responses



10. How easy is it to understand and use the system's main features as a new user?
10 responses