A Mini Project Report on

COLLEGE GATE AUTOMATION SYSTEM

Submitted in partial fulfillment of the requirement for the award of the degree of
Bachelor of Technology in Computer Science and Technology

By

D. Himateja Reddy (21251A3633)

T. Sai Nikhitha (21251A3660)

V. Sanjana (21251A3663)

Under the Guidance of

Mrs. Y. Rajalakshmi

Asst. Prof, CST

G. Narayanamma Institute of Technology and Science
(For Women)
(AUTONOMOUS)
Approved by AICTE, New Delhi & Affiliated to JNTUH, Hyderabad
Accredited by NBA & NAAC
Shaikpet, Hyderabad – 500104, TS.

July 2024

Declaration by Candidate

We hereby affirm, to the best of our knowledge and belief, based on observations, reviews, testing of the project and upon reports submitted by us, this mini project entitled **College Gate Automation system** is substantially complete and operable. The execution of the **College Gate Automation system** Project adheres strictly to the guidelines issued by the department.

Name of the candidate **Signature**

D. Himateja Reddy

T. Sai Nikhitha

V. Sanjana

G. NARAYANAMMA INSTITUTE OF TECHNOLOGY & SCIENCE

(AUTONOMOUS)

(For Women)

(Sponsored by G. Pulla Reddy Charities Trust, Hyderabad)
Accredited by NBA (UG : ECE, EEE, CSE & IT, PG : CSE, CNIS, PEED) & NAAC,
NIRF Ranking 2022: Rank Band in Engineering : 251-300
Approved by AICTE & Affiliated to JNTUH

CERTIFICATE

This is to certify that mini project report entitled **College Gate Automation system Forum** is bonafide work done

By

Name of the candidate	Registration Number
1. **D. Himateja Reddy**	**21251A3633**
2. **T. Sai Nikhitha**	**21251A3660**
3. **V. Sanjana**	**21251A3663**

under the guidance **Mrs. Y. Rajalakshmi, Asst. Professor** during January 2024 to July 2024, in partial fulfilment for the award of degree in B. Tech in Computer Science and Technology, from G. Narayanamma Institute of Technology & Science.

Internal Guide

Mrs. Y. Rajalakshmi

Asst. Professor CST

HOD IT

Dr. S. Ramacharan

8-1-297/2/I, Shaikpet, Hyderabad - 500 104, Telangana
✆: 040-2956 5856 / 2956 7756 E-mail : principal@gnits.ac.in Website : www.gnits.ac.in

ACKNOWLEDGEMENT

The successful completion of our mini project would not be possible without the timely help and guidance rendered by many people. We would like to take this opportunity to thank all of them from the bottom of our heart.

We express our sincere thanks to **Dr. K. Ramesh Reddy**, Principal, G. Narayanamma Institute of Technology and Science for providing us with all the resources and equipment without which this mini project would not be possible.

We express our gratitude to **Dr .S. Ramacharan**, Head of the Department of Information Technology, G. Narayanamma Institute of Technology and Science for his support which helped us to carry out the mini project work.

We profoundly indebted to our project coordinators **Mrs. V. Usha**, Asst. Professor, Information Technology and **Mrs. K. Madhavi**, Asst. Professor, Information Technology for their prompt guidance, support, and oversight, which kept us inspired the entire time. Finally, we extend our heartfelt thanks to our project internal guide, **Mrs. Y. Rajalakshmi**, Asst. Professor, Information Technology whose guidance steered us in the right direction during our project.

ABSTRACT

Automatic gate is one of the most useful things to use in colleges and schools. It is aimed to develop and evaluate an Automated Gate Pass System designed to keep track of the students, employees, and visitors passing through the campus gate. Automatic gates are important and very useful because it helps save time, reduces the human force applied to the opening and closing of the manual gate which saves energy and also saves gate operators from health hazards caused by exposing themselves to harsh weather conditions in the course of operating the manual gate and also improve the management of access to restricted areas through an automated gate control network. College Gate Automation System addresses identification system for vehicles using RFID. The owner is given his RFID tag to be pasted on a vehicle. When vehicle passes through Gate it is classified as a passenger based on its Unique Identification Number (UIN). Vehicle's In & Out time will be recorded into the Database. Thus, the system contributes in securing and monitoring the students, employees, and visitors; thereby generating due and timely feedback to the administration.

CONTENTS

1.Introduction and Problem Analysis

1.1 General Description

The college gate automation system aims to streamline the entry and exit process of vehicles and pedestrians into and out of the college premises. The current manual system is prone to inefficiencies, delays, and security risks. Hence, there is a need to develop an automated solution that enhances security, improves efficiency, and provides convenient access control for students, faculty, staff, and authorized visitors.

The College Gate Automated System is designed to enhance security, access control, and administrative efficiency at college entrances. It integrates RFID/smart card readers for identity verification & vehicle access. Boom barriers and bollards manage vehicle entry, while visitor management is facilitated through a pre-registration system and on-site kiosks. An administrative dashboard offers real-time monitoring, reporting, analytics, and user management, while automated notifications and an intercom system enhance communication. Benefits include enhanced security, operational efficiency, accurate record keeping, and convenience, making it scalable for small colleges to large universities.

Additional features include integration with campus databases for cross-referencing identities, customizable access levels and permissions for different user groups, and emergency protocols for lockdowns or evacuations. This system supports scalability to accommodate the needs of small colleges and large universities alike, offering a robust, user-friendly, and secure solution for managing campus access. Benefits encompass enhanced security, reduced congestion at entry points, operational efficiency, convenience for users, and accurate, easily accessible records, ensuring a safe and efficient campus environment.

1.2 Problem Statement

The primary challenge faced by colleges and universities is ensuring a secure, efficient, and user-friendly access control system at their campus entrances. Traditional manual methods of verifying the identity of students, staff, visitors, and vehicles are time-consuming, prone to human error, and often lead to congestion and security vulnerabilities. Moreover, managing large volumes of entry and exit data manually is cumbersome and inefficient, making it difficult to maintain accurate records and swiftly respond to security incidents.

Colleges need a scalable solution that can integrate seamlessly with their existing infrastructure, provide real-time monitoring and reporting, enhance communication, and improve overall security without compromising the convenience of users. This includes effectively managing different access levels for various user groups, handling temporary access for visitors, and ensuring vehicle entry is secure and efficient. The solution must also be capable of generating detailed reports and analytics for administrative purposes while being flexible enough to adapt to the unique needs of each institution.

Institutions, mainly educational campuses, are often faced with the challenge of managing vehicular access efficiently while ensuring security and convenience for students, faculty, and visitors. Traditional manual gate systems can be labor-intensive, prone to errors, and may not provide adequate security measures. In response to these challenges, the development of an automated gate system tailored specifically for college campuses becomes imperative. This system provides a flexible, scalable and cost-effective solution for security access control. This system reads the RFID(Radio Frequency Identification) tag ID, validates against a database, and opens the gate automatically for authorized users. Passive RFID tags are used which don't require batteries and are low cost. It logs user check-in and check-out events along with details like time and date.

1.3 Scope of the Project

This is a practical application for future uses such as Smartcart can be interfaced with wireless technologies to make it completely portable in the near future. A low cost RFID scanner can be manufactured and used which can scan multiple tags (products) simultaneously for faster processing and lesser resources. Automatic scanning& availability of products can be introduced.

The scope of the College Gate Automated System project encompasses the design, implementation, and integration of advanced access control technologies to enhance security and efficiency at campus entrances. This includes the installation of RFID/smart card readers, biometric scanners, QR code/barcode scanners, and automated license plate recognition systems for seamless identity and vehicle verification. This project aims to ensure a smooth transition from existing systems, with a phased deployment strategy and scalability to accommodate future growth, along with ongoing support and continuous improvement based on user feedback and technological advancements.

Comprehensive user management will involve issuing RFID/smart cards, registering biometric data, and defining access levels and permissions for different user groups. An automated notification for the entry of the vehicle into/exit of the gate will be sent to the authorized person with respect to the college institution. The projects extends its scope with respect to the college management or universities etc.

1.4 Objectives

- Register new users and encode their information into an RFID tag.
- Implement a security system for secured zones, allowing access only to authorized individuals.
- Utilize passive RFID technology to activate, verify, and authorize users, opening doors in real-time.
- Use RFID to automatically record attendance of students and staff.
- Achieve potential savings in administrative and security operations.

1.5 Organization of Project Report

CHAPTER 1: INTRODUCTION: This Chapter includes General Description of the Project. Objectives (Major and Minor) and scope of the project, Project Definition, Technical and Operational Feasibility.

CHAPTER 2: LITERATURE SURVEY: This Chapter includes various Existing Projects Approaches /Systems through analyzing various surve papers, Drawbacks in Existing Systems and Introduction towards motivation for Proposed System.

CHAPTER 3: REQUIREMENT SPECIFICATION: This Chapter includes Overall Description of the Project along with use –case diagram, Functional, Non-Functional Requirements Specification of stakeholders involved Software and Hardware Specifications of the Project.

CHAPTER 4: IMPLEMENTATION: This Chapter includes explanation of methodology involved along with flow chart, System Architecture, Description of the various Modules with code.

CHAPTER 5: TESTING: This Chapter consists of Test-cases to be performed in order to evaluate the system and its components with the intent to find whether it satisfies the specified requirements or not.

CHAPTER 6: RESULT AND CONCLUSION: This chapter consists of Analysis of the performance and result of the project by showcasing the execution of project through screenshots and portraying the conclusion of the project.

2. LITERATURE SURVEY

2.1 Existing Approaches

Automatic gate control for highly secure organization using RFID and GSM Technology (V.Sri Vaishnavi , V.Srinaya , T.Preethi & S. Aishwaya)

This review paper provides a comprehensive overview of the current state of research on an automated gate for high secure. The main objective of this research is to the intimate fake person entering into a highly secured organization like Hospitals, Schools, Industries and Colleges using RFID and GSM Technology. Traditionally, most of the people used to enter into secured places to steal or create unwanted problems which violating the terms and condition of the organization. In this regard, the proposed research article claims to forward fake person to the corresponding or authorized person in the same instance of time. Thereby, the accomplishment of the aforesaid security system is maintained by RFID Tag-based database by the organization. A novelty approach restricts unauthorized people from getting into the secured organization or zone. The suggested module in this proposed research works more efficiently which suits real-time execution.

Smart Gate (Prof. Hemlata Ohal & Sujata Jadhav)

This review paper provides a comprehensive overview of the current state of research on an Automated Gated System, an introduction of the common world to the Digital and Automated world. Automation is term which has made the lives of the population quite easier. It reduces human effort and the errors made by humans. It connects the society with technology which makes the society more advanced and developed. In common world the gates works as a mechanism for security, but this security can be compromised when it is being provided by human. So using technology in this case would provide more security than human, also it will never be compromised and the dependency is least while working with technology. y. Automated gate opening system is a step of combining manual human work with technological advancements. As the trend, which is seen in the society is the security guard opening the gates or the gate automatically opening as someone enters. Thus in this paper we have proposed a system which includes combination of sensor technology and IoT (Internet of Things).

Using this system one can control the gate through his Smartphone or it could be operated without any manual work and work fully automatically.

Automatic gate based on Arduino microcontroller UNO R3 (R Arrahman)

This research aims to design and implement a circuit that serves to open and close the gate automatically with remote control through a smartphone. It uses the Bluetooth HC-05 as a transmission between the smartphone and the Arduino Uno R3 microcontroller. To control arduino microcontrollers, the C programming language is used using Arduino software. . First the smartphone must be connected with a connection between Bluetooth HC-05 and Bluetooth on the smartphone, after connecting the user can open a special application to control the movement of the gate closes or opens also stop the movement of the gate. When the user presses the button in the application, the data contained in the button will be sent via Bluetooth to the microcontroller for further execution. If the user presses the button to open then the DC motor as the gate mover will automatically move to open the gate. Stopping the movement of the gate can be done by pressing the existing button applied.

Hardware Design of Queuing Free Environmental Friendly Automatic Toll Gate Using RFID (Darjat & A. F. Listyono)

This research aims to improve the quality of service of the toll gates by developing a queuing free environmental friendly automatic toll gates. Instead of debit card to identify the toll customers and do the payment, the proposed system uses a noncontact technology that commonly referred as Radio Frequency Identification. The vehicle is identified by the systems just as it is passing through the toll gate. Regardless the gates are manual or automatic, every vehicle should stop for a while to finish the transaction. The more vehicles come, the longer queue be. The longer queue, the more wasting fuel consumption and the higher air pollution be **.** Next, a payment notification is sent to the driver’s hand phone via short message service. It replaces the need of paper and ink and eliminates paper trashes around the toll gates. This paper presents the hardware development of the proposed system.

RFID based Smart Automatic Vehicle Management System for Healthcare Applications (B.Pavithra, S.Suchitra & P.Subbulakshmi)

This review paper provides a comprehensive overview of the current state of research on Smart automatic vehicle management system using RFID technology is proposed. This work conglomerates the widely used image processing technique with the trending Internet of Things (IoT) paradigm. The use of RFID reader in the main gate to read the tag of vehicle and the information will be sent to the management, once the vehicle enters the school campus and abates trespassing. This proposed work is applied in real-time scenario, which is mainly helpful in contributing to the enhanced tracking of school children safety and monitoring proper functioning of vehicles without any malfunctioning and curtailing further complications. The vehicle emission monitoring is also a key factor, which is implemented by identifying the overheating in vehicle through temperature sensor and the smoke problem (vehicle emitting smoke) through the use of gas sensor and immediate necessary actions will be taken by the driver or the management to ensure proper functioning of the vehicle**.** This paper is a valuable resource for researchers and practitioners interested in the field of IOT.

2.2 Drawbacks in Existing System

Despite its advantages, the automated gate access control system using Arduino, RFID, and GSM technology may have several drawbacks:

1. **Cost of Implementation**: Initial setup costs, including hardware (such as RFID scanners and GSM modules), installation, and integration with existing infrastructure, can be substantial, particularly for large-scale deployments in industrial settings.
2. **Maintenance Requirements**: The system requires regular maintenance to ensure proper functionality of RFID scanners, GSM modules, and other components. This ongoing upkeep adds to operational costs and demands technical expertise.
3. **RFID Interference**: Environmental factors like metal interference or electromagnetic interference can affect RFID tag detection and scanning accuracy, potentially leading to unreliable performance.

4. **Security Vulnerabilities:** While RFID technology offers secure authentication, it is not immune to hacking or cloning attempts. Sophisticated attackers may attempt to intercept or spoof RFID signals to gain unauthorized access.
5. **Dependence on GSM Network**: Reliance on GSM networks for real-time alerts and remote access control introduces vulnerabilities related to network coverage, connectivity issues, and potential delays in communication.
6. **User Training and Adoption**: Users and administrators may require training to effectively operate and manage the system, potentially leading to initial resistance or learning curves.
7. **Integration Complexity**: Integrating the system with existing security systems, such as CCTV or access control software, can be complex and may require specialized technical knowledge.

Addressing these drawbacks requires careful planning, robust security measures, ongoing maintenance, and proactive management to ensure the system meets its intended security and operational objectives effectively.

2.3 Motivation for Proposed System

The automated gate access control and security monitoring system, centered around Arduino technology and leveraging RFID for identification alongside GSM for alerts, represents a comprehensive solution tailored for enhancing security and operational efficiency in various settings.

Authorized vehicles equipped with RFID tags are seamlessly granted entry through the gate upon validation against a centralized database. This system ensures swift and secure access management, minimizing delays and optimizing traffic flow within residential, commercial, or industrial premises.

User check-in and check-out events are meticulously logged within the system, capturing crucial details such as timestamps and dates. This logging capability not only aids in monitoring entry and exit activities but also serves as a valuable resource for auditing, analytics, and operational planning purposes.

This flexibility allows the system to adapt to evolving security needs and technological advancements seamlessly.

For visitor management, RFID stickers or tags are provided for vehicles, affixed temporarily to windshields using adhesive. This approach ensures that authorized visitors can access the premises conveniently while maintaining security protocols. Security personnel manage the issuance of RFID stickers to visitors, following instructions from owners or authorized personnel to streamline visitor access procedures efficiently.

Addressing these challenges requires meticulous planning, regular system audits, and proactive maintenance to uphold robust security measures and operational efficiency. By leveraging the strengths of Arduino, RFID technology, and GSM communication, this automated gate access control and security monitoring system aims to provide a secure, scalable, and user-friendly solution for effectively managing access and enhancing security in diverse environments.

Key components of the system include:

The automated gate access control and security monitoring system based on Arduino, RFID, and GSM incorporates several key components to ensure its functionality and effectiveness:

1. Arduino Microcontroller: Acts as the central processing unit for the system, handling data processing, decision-making logic, and interfacing with other components.
2. RFID Readers and Tags: RFID readers are used to scan RFID tags affixed to vehicles or carried by individuals. Tags contain unique identifiers that are validated against a database to grant access permissions.
3. Centralized Database: Stores information about authorized users, vehicles, access permissions, and logging of entry and exit events. The database ensures quick verification and retrieval of information during access control operations.
4. RFID Stickers/Tags for Visitors: Temporary RFID tags or stickers affixed to visitor vehicles allow controlled access based on instructions from authorized personnel or owners, ensuring streamlined visitor management processes.

3. Requirement Specification and Design

3.1 Overall Description of the project

RFID (Radio Frequency Identification) provides a fast, secure and convenient technology for automated access control applications. Passive RFID tags are used which don't require batteries and are low cost. The system reads the RFID tag ID, validates against a database, and opens the gate automatically for authorized users. It logs user check-in and check-out events along with details like time and date. The modular architecture allows integrating sensors, alarms, GSM modules for enhanced functionality.

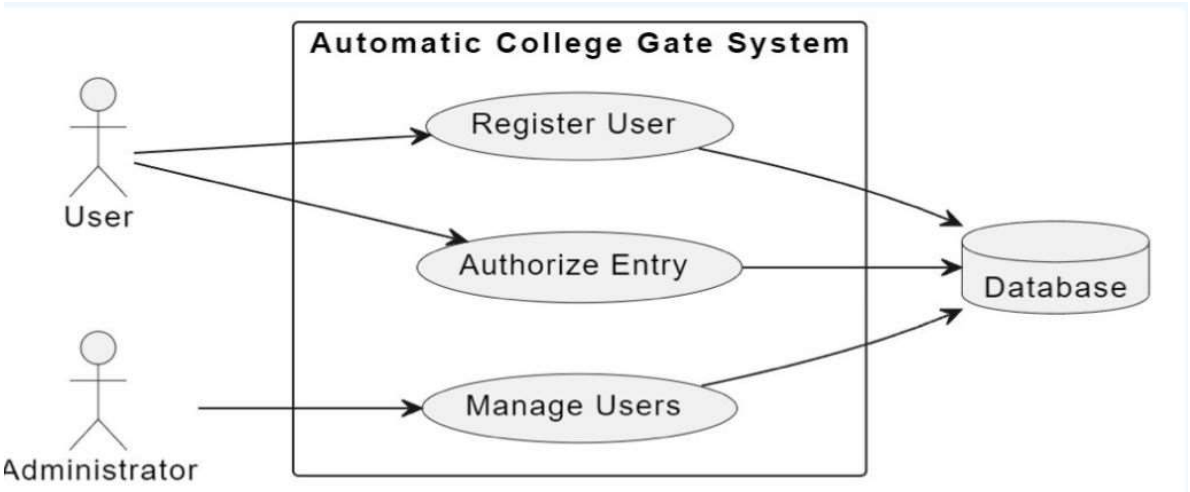
The project aims to develop an advanced automated gate access control and security monitoring system using Arduino, RFID technology, and GSM communication for deployment in residential, commercial, and industrial environments.

Key components include Arduino microcontrollers for system control, RFID readers and tags for identification, a GSM module for real-time communication of alerts and notifications, and optional environmental sensors for enhanced monitoring capabilities

Visitor management is streamlined with temporary RFID tags or stickers issued to authorized visitors, affixed to vehicles for controlled access. The system includes provisions for user-friendly interfaces for administrators, ensuring efficient management of access permissions, system configurations, and monitoring of security events.

Challenges such as initial setup costs, maintenance requirements, and potential environmental factors influencing RFID signal integrity are addressed through meticulous planning and proactive maintenance. The project aims to deliver a robust, reliable, and user-friendly solution that enhances security measures, optimizes operational efficiency, and supports comprehensive access management in diverse settings.

Use Case Diagram:



The system reads the RFID tag ID, validates against a database, and opens the gate automatically for authorized users. It logs user check-in and check-out events along with details like time and date. User activities, including check-ins and check-outs, are meticulously logged for monitoring and audit purposes.

The basic working of the automated gate access control system begins with the RFID reader scanning the RFID tag presented at the gate. The Arduino microcontroller then compares the tag's unique identifier with entries in the centralized database of authorized users and vehicles. If the tag is valid and matches an entry in the database, the gate is automatically unlocked to allow entry. In cases of invalid or unrecognized tags, the system triggers an alarm to alert security personnel or administrators of a potential unauthorized access attempt.

Simultaneously, the system updates usage logs in the database, recording details such as the timestamp of each entry and exit event for audit and monitoring purposes. These logs ensure accurate tracking of access activities and provide a historical record of system usage. Additionally, the status of access attempts and any triggered alarms, along with real-time alerts, are displayed on an LCD screen or sent via SMS to designated recipients, ensuring immediate awareness and response to security events. This integrated approach enhances security measures, ensures operational

transparency, and supports effective access management in residential, commercial, or industrial environments.

The basic working is:

1.RFID Reader scans tag

2.Micro-controller verifies tag ID with database

3.If valid, unlocks gate, else triggers alarm.

4.Usage logs updated in database

5.Status and alerts shown on LCD display and SMS

3.2 Functional & Non-Functional Requirements Specification

Functional Requirements

1. User Registration:
    - The system shall allow registration of students, employees, and visitors.
    - Each user shall be assigned a unique RFID tag with a Unique Identification Number (UIN).
2. RFID Tag Reading:
    - The system shall be capable of reading RFID tags from a predefined distance.
    - The system shall recognize the RFID tag and authenticate the user.
3. Gate Control:
    - The system shall automatically open the gate when a valid RFID tag is detected.
    - The system shall prevent gate operation for invalid or unregistered RFID tags.
4. Time Logging:
    - The system shall log the entry and exit times of vehicles.
    - The logged data shall be stored in a secure database.
5. Access Control:
    - The system shall restrict access to certain areas based on user roles (e.g., student, employee, visitor).
    - The system shall allow administrators to define and modify access permissions.
6. Monitoring and Alerts:

- The system shall monitor the gate operations and send alerts for unauthorized access attempts.
- The system shall generate real-time alerts for any system malfunctions.

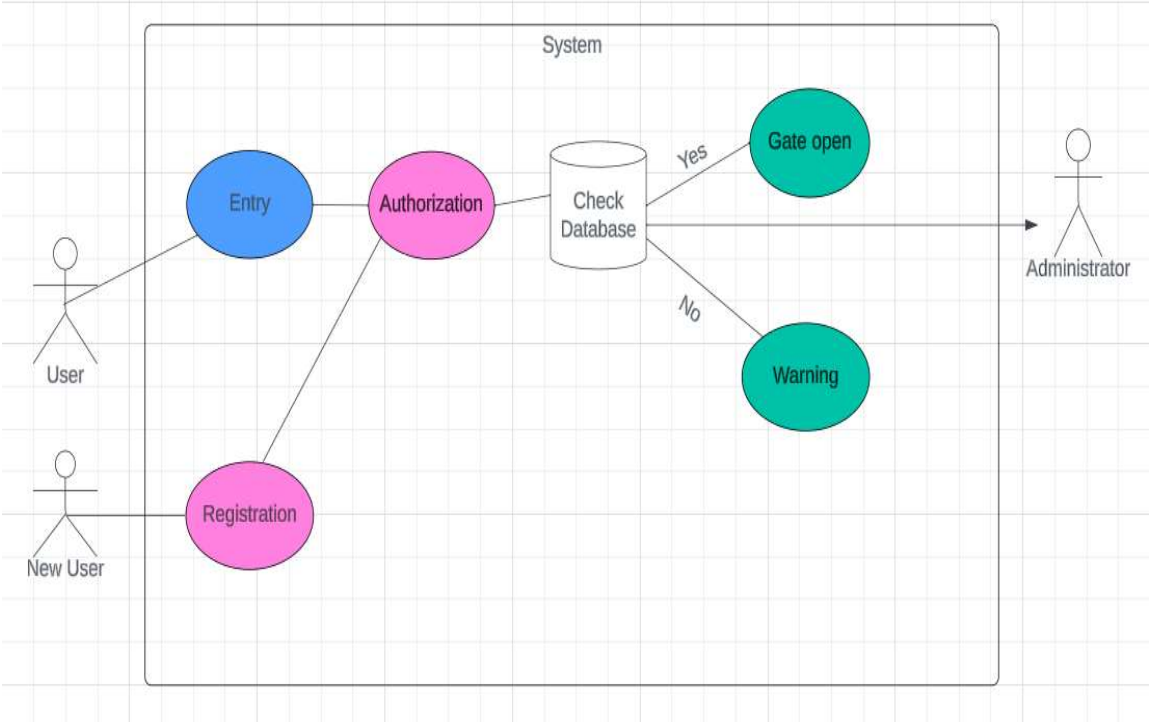
7. Report Generation:
    - The system shall generate daily, weekly, and monthly reports on gate usage.
    - The system shall provide detailed reports on specific users or groups of users.

Non-Functional Requirements

1. Performance:
    - The system shall have a response time of less than 2 seconds for RFID tag detection and gate operation.
    - The system shall be capable of handling a high volume of users (up to 1000 entries/exits per hour).
2. Reliability:
    - The system shall have an uptime of 99.9%.
    - The system shall provide backup mechanisms for power and data loss scenarios.
3. Security:
    - The system shall use encryption for data transmission between RFID readers and the database.
    - The system shall implement access controls to protect sensitive data.
4. Scalability:
    - The system architecture shall support integration with other security and monitoring systems.
5. Usability:
    - The system shall have a user-friendly interface for administrators and security personnel.
    - The system shall provide clear and concise instructions for users interacting with the gate.
6. Maintainability:
    - The system shall be designed for easy maintenance and troubleshooting.

- The system shall provide diagnostic tools for identifying and resolving issues.

These requirements provide a comprehensive overview of the expected functionality



This use case diagram illustrates the interactions between different actors and the system components in an Automated Gate Pass System.

Actors

1. User
    - Represents any individual (student, employee, or visitor) who uses the automated gate system for entry.
2. New User
    - Represents a person who needs to be registered into the system (new student, employee, or visitor).
3. Administrator
    - Represents the person responsible for overseeing the system, managing user registrations, and handling any warnings or alerts.

Use Cases

1. Entry
    - Actor: User
    - Description: This use case involves the user attempting to enter through the gate by presenting their RFID tag.
    - Flow:
        1. The user presents their RFID tag.
        2. The system detects the RFID tag and initiates the Authorization process.
2. Authorization
    - Actor: System
    - Description: This use case involves the system validating the user's RFID tag against the database.
    - Flow:
        1. The system checks the database for the user's information.
        2. If the RFID tag is valid, the system authorizes entry.
        3. If the RFID tag is invalid, the system denies entry and issues a warning.
3. Registration
    - Actor: New User
    - Description: This use case involves the registration of a new user into the system.
    - Flow:
        1. The new user provides their details to the system.
        2. The system registers the new user and assigns an RFID tag.
4. Check Database
    - Actor: System
    - Description: This use case involves the system querying the database to verify the user's RFID tag.
    - Flow:
        1. The system accesses the database to check the user's RFID tag and associated permissions.

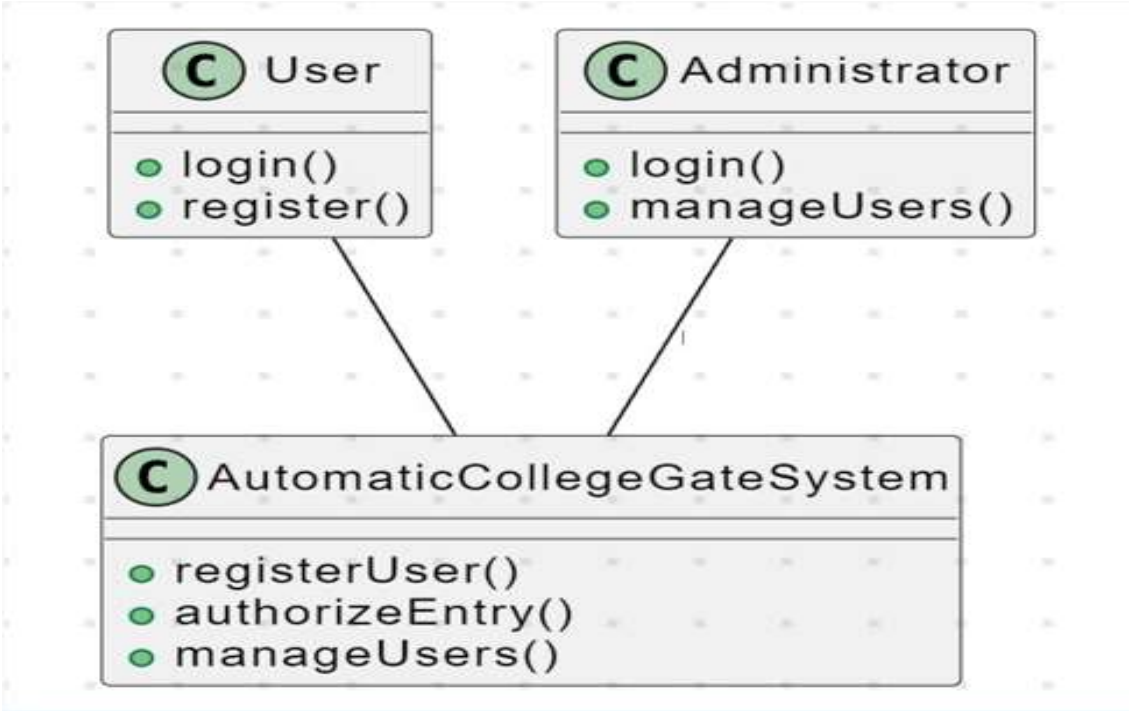
5. Gate Open
    - Actor: System
    - Description: This use case occurs when the user's RFID tag is validated, and the system opens the gate.
    - Flow:
        1. The system receives a positive authorization.
        2. The system opens the gate for the user.
6. Warning
    - Actor: System
    - Description: This use case occurs when the user's RFID tag is not validated, and the system issues a warning.
    - Flow:
        1. The system receives a negative authorization.
        2. The system issues a warning and logs the attempt.
        3. The administrator is notified of the unauthorized attempt.

System Flow

- Entry leads to Authorization.
- Authorization involves Check Database.
- Based on the database check, the system either proceeds to Gate Open or Warning.
- Registration is initiated by a New User and managed by the system.
- Administrator is involved in overseeing warnings and managing the system.

This diagram provides a clear overview of the interactions and processes involved in managing automated gate access using RFID technology.

CLASS DIAGRAM :



The class diagram depicts the structure of the Automatic College Gate System, focusing on its main components and their relationships.

Classes

1. User
    - Description: Represents a general user of the system, which can be a student, employee, or visitor.
    - Methods:
        - login(): Allows the user to log into the system.
        - register(): Allows a new user to register into the system.
2. Administrator
    - Description: Represents an administrator who has additional privileges to manage the system.
    - Methods:
        - login(): Allows the administrator to log into the system.
        - manageUsers(): Allows the administrator to manage user accounts (e.g., add, remove, or update users).
3. AutomaticCollegeGateSystem
    - Description: Represents the core system responsible for handling gate operations, user registrations, and authorizations.

- Methods:
  - registerUser(): Registers a new user into the system.
  - authorizeEntry(): Authorizes a user's entry based on their RFID tag.
  - manageUsers(): Manages user accounts and their access rights.

Relationships

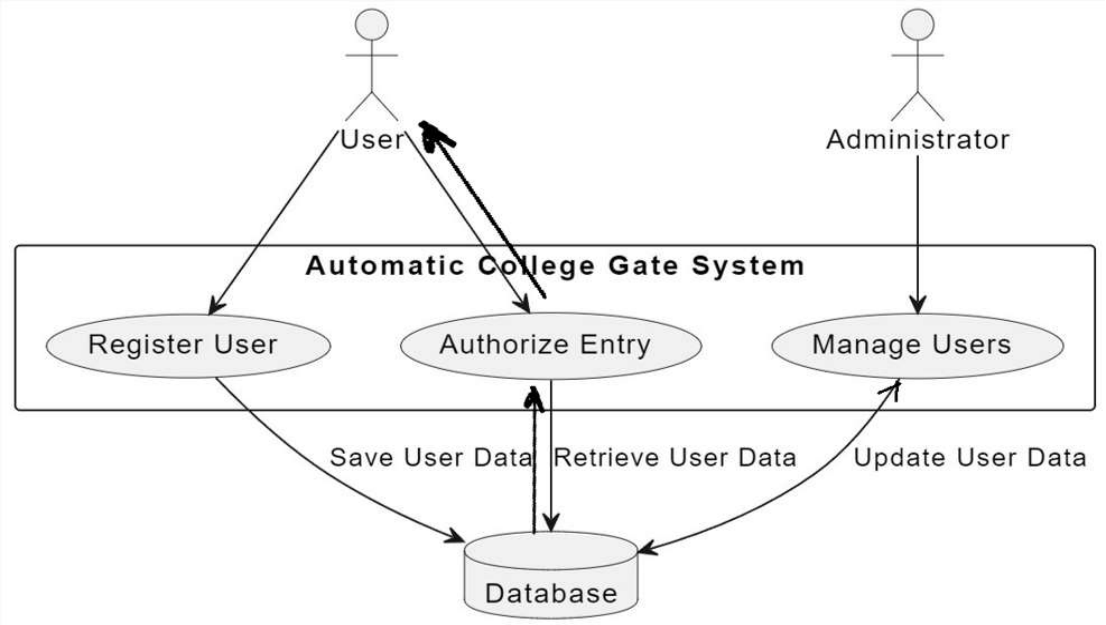
- User and AutomaticCollegeGateSystem
  - The User class is connected to the AutomaticCollegeGateSystem class, indicating that users interact with the system to perform actions such as logging in and registering.
- Administrator and AutomaticCollegeGateSystem
  - The Administrator class is connected to the AutomaticCollegeGateSystem class, showing that administrators have special privileges to manage users within the system.

Class Interactions

1. User Interactions:
   - A User can log into the system using the login() method.
   - A new User can register themselves using the register() method, which in turn interacts with the registerUser() method of the AutomaticCollegeGateSystem to add the new user.
2. Administrator Interactions:
   - An Administrator can log into the system using the login() method.
   - An Administrator can manage user accounts using the manageUsers() method, which interacts with the manageUsers() method of the AutomaticCollegeGateSystem to perform necessary user management operations.
3. System Operations:
   - The AutomaticCollegeGateSystem is responsible for the core functionalities:
     - registerUser(): Handles the registration of new users.
     - authorizeEntry(): Authorizes user entry by validating their RFID tag against the system's database.
     - manageUsers(): Allows the administrator to manage the user accounts and their access privileges.

This diagram provides a clear representation of the system's structure and the interaction between users, administrators, and the core system.

INTERACTION DIAGRAM:



This interaction diagram illustrates the flow of activities and interactions between different actors and components in the Automatic College Gate System.

Actors

1. User
    - Represents any individual (student, employee, or visitor) who uses the automated gate system for entry.
2. Administrator
    - Represents the person responsible for overseeing the system, managing user registrations, and handling updates to user data.

System Components

1. Automatic College Gate System
    - The main system that handles user registration, entry authorization, and user management.
2. Database
    - The central storage where user data is saved, retrieved, and updated.

Use Cases

1. Register User
    - Actor: User

- Description: The process by which a new user registers into the system.
- Interactions:
  - The user interacts with the Register User component of the Automatic College Gate System.
  - The system saves the new user's data into the Database.

2. Authorize Entry
   - Actor: User
   - Description: The process of authorizing a user’s entry through the gate.
   - Interactions:
     - The user attempts to enter by interacting with the Authorize Entry component.
     - The system retrieves user data from the Database to validate the user's RFID tag.
     - Based on the retrieved data, the system either authorizes the entry or denies it.
3. Manage Users
   - Actor: Administrator
   - Description: The process of managing user accounts, which includes adding, removing, or updating user data.
   - Interactions:
     - The administrator interacts with the Manage Users component of the Automatic College Gate System.
     - The system updates the user data in the Database accordingly.

System Flow

1. Register User Flow:
   - A new User initiates the registration process.
   - The Automatic College Gate System registers the user by saving their data into the Database.
2. Authorize Entry Flow:
   - A User attempts to enter through the gate.
   - The Automatic College Gate System interacts with the Database to retrieve the user’s data.
   - If the data matches, the entry is authorized.
3. Manage Users Flow:

- The Administrator manages user data.
- The Automatic College Gate System updates the Database with the new or modified user data.

This interaction diagram provides a clear overview of how users and administrators interact with the Automatic College Gate System and how the system interacts with the database to handle user registration, entry authorization, and user management. The arrows indicate the flow of data and actions between the actors, system components, and the database, illustrating the process of saving, retrieving, and updating user data.

3.4 S/w and H/w Requirements

- **RFID Reader Software:** The RFID reader software is crucial for interpreting the data transmitted by RFID tags. This software enables the RFID reader to identify and differentiate between various tags. It includes APIs for integration with other systems, ensuring smooth communication between the reader and the gate control system. This software must be reliable and capable of processing multiple readings simultaneously to handle high traffic efficiently.

- **Gate Control Software:** This software controls the physical opening and closing of the gate based on the input received from the RFID reader. It integrates with both the reader software and the database to verify access permissions in real-time. The gate control software must be responsive and reliable, ensuring that authorized vehicles and individuals can pass through without delay while unauthorized attempts are promptly denied.

- **User Interface (UI):** A user-friendly interface is essential for administrators to monitor and manage the automated gate system. This can be a web-based or mobile application providing real-time data on gate activities. The UI should include a dashboard displaying entry and exit logs, alerts for unauthorized access, and options to manage RFID tags and access permissions.

- **Notification System:** The notification system is responsible for alerting administrators to any unauthorized access attempts or system issues. It can

send notifications via email, SMS, or app alerts, ensuring that the administration is immediately aware of any potential security breaches or technical problems. This system helps in maintaining a high level of security and prompt response to any incidents.

- **Security Software:** Protecting the automated gate system from external threats is vital. Security software, including firewalls and antivirus programs, safeguards the system against hacking, malware, and other cyber threats. Additionally, data encryption ensures that all communication within the system is secure, preventing unauthorized access to sensitive information.

Hardware Requirements

- **RFID Readers:** RFID readers are the backbone of the automated gate system, responsible for reading the unique identifiers from RFID tags. These readers must have a suitable read range to detect tags on vehicles and individuals as they approach the gate. Durability and weather resistance are also crucial, especially for outdoor installations.

- **RFID Tags:** Each vehicle and individual requiring access is issued a unique RFID tag. These tags can be passive, relying on the reader's signal for power, or active, with their own power source for longer read ranges. The tags must be securely attached to vehicles or carried by individuals to ensure consistent and accurate readings by the RFID readers.

- **Automated Gate Barrier:** The automated gate barrier is a mechanical system that physically opens and closes the gate based on commands from the control software. This barrier needs to be robust and able to withstand frequent use and varying weather conditions. It must also operate smoothly and quickly to prevent traffic congestion at the gate.
- **Controllers:** Controllers, such as microcontrollers or programmable logic controllers (PLCs), are used to interface with the RFID reader and control the gate mechanism. These devices process the signals

from the RFID reader and execute the appropriate actions, such as opening or closing the gate. Reliable controllers ensure the system's responsiveness and accuracy.

- **Networking Equipment:** Networking equipment, including routers, switches, and cabling, is necessary to connect all components of the automated gate system. This infrastructure enables seamless communication between the RFID readers, controllers, database, and user interface. A stable and secure network is essential for the system's overall performance and reliability.

- **Computers/Servers:** Dedicated computers or servers are required to run the control software, database, and user interface. These machines should have sufficient processing power and storage capacity to handle the system's demands. Reliable hardware ensures that the system can operate continuously without performance issues or downtime.

- **Power Supply:** An uninterruptible power supply (UPS) is crucial for maintaining system stability during power outages. It ensures that the RFID readers, gate barriers, and other critical components remain operational. Additionally, backup generators can provide extended power support, ensuring the system's reliability even during prolonged outages.

- **Security Cameras:** Installing security cameras at the gate adds an extra layer of surveillance, recording all activities for later review. These cameras can integrate with the control software, allowing real-time monitoring and providing visual confirmation of entries and exits. Security cameras enhance the overall security of the automated gate system

4.Implementation

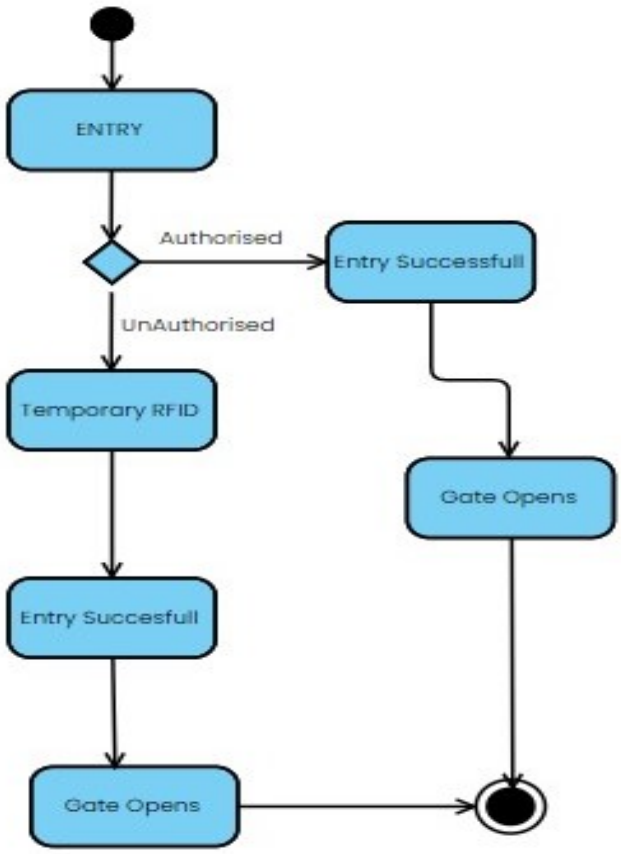
4.1 Methodology

1. Requirement Analysis:
    - Objective: Gather and analyze the requirements for the Automated Gate Pass System.
    - Tasks:
        - Conduct stakeholder meetings (administrators, security personnel, students, employees, visitors).
        - Document functional and non-functional requirements.
        - Define scope and constraints.
2. System Design:
    - Objective: Design the architecture and components of the system.
    - Tasks:
        - Design system architecture (hardware and software).
        - Define data flow and system integration points.
        - Create database schema for logging and managing data.
        - Design user interface for administrators and users.
3. Development:
    - Objective: Develop the system components.
    - Tasks:
        - Develop RFID reader integration.
        - Implement Thai ID card detection module.
        - Develop gate control mechanism.
        - Implement data logging and storage system.
        - Develop monitoring and alert system.
        - Create report generation module.
4. Testing:
    - Objective: Ensure the system meets the specified requirements and works correctly.
    - Tasks:

        - Conduct unit testing for individual components.
        - Perform integration testing to ensure components work together.
        - Execute system testing to validate overall functionality.
        - Carry out user acceptance testing (UAT) with stakeholders.
5. Deployment:
    - Objective: Deploy the system to the live environment.
    - Tasks:
        - Set up hardware (RFID readers, gates, servers).
        - Install and configure software components.
        - Migrate data and configure database.
        - Train administrators and security personnel.
6. Monitoring and Maintenance:
    - Objective: Ensure the system operates smoothly and remains updated.
    - Tasks:
        - Monitor system performance and uptime.
        - Respond to alerts and troubleshoot issues.
        - Perform regular maintenance and updates.
        - Gather feedback and make necessary improvements.

FLOWCHART:

Here's the flowchart representing the methodology:

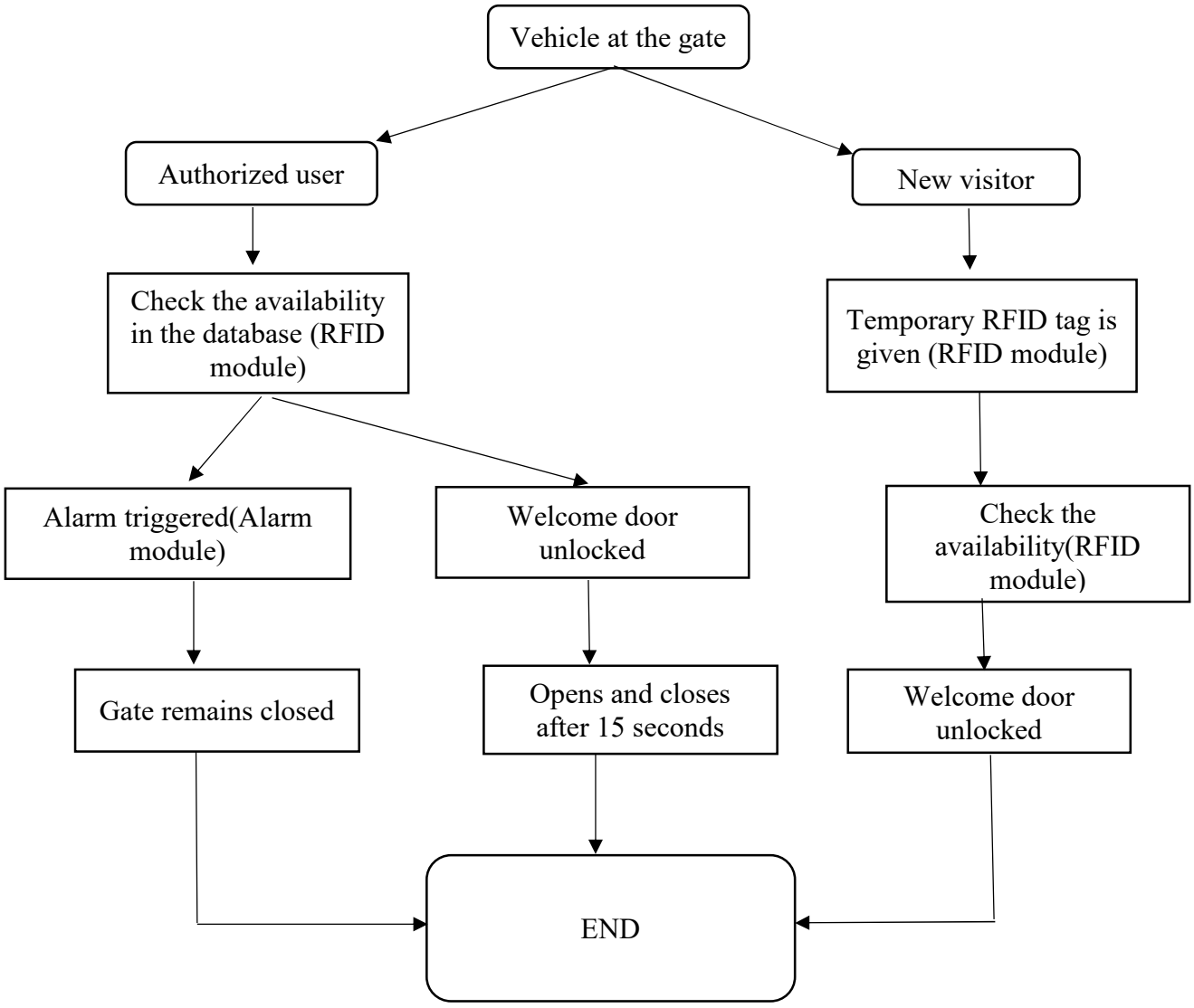


1. **Vehicle Approaches the Gate:**
    - The RFID reader detects the RFID tag on the vehicle and reads the unique ID.
2. **ID Verification:**
    - The unique ID is sent to the microcontroller, which checks it against the database.
    - If the ID is valid, the microcontroller sends a signal to the gate control module to open the gate.
    - If the ID is invalid, the microcontroller triggers the alarm module.
3. **Gate Operation:**
    - The gate control module opens the gate to allow the vehicle to pass.

- The gate closes after a specified time interval.

4. **Alerts and Notifications:**
   - If an unauthorized access attempt is detected, the GSM module sends an alert to the relevant authorities.
   - The alarm module provides immediate visual/audio alerts on-site.

4.2 System Architecture



Entities in the System Architecture

1. **Vehicle at the Gate:**

- This represents the starting point where a vehicle arrives at the college gate. The vehicle could belong to an authorized user or a new visitor.

2. **Authorized User:**
   - This branch of the flowchart is for users who already have authorization to access the campus. These users have an RFID tag that is recognized by the system.
3. **New Visitor:**
   This branch of the flowchart is for visitors who do not have pre-authorization. New visitors will need to be issued a temporary RFID tag to access the campus.
4. **Check the Availability in the Database (RFID Module):**
   - This step involves the RFID module checking if the RFID tag presented by the user or visitor is available in the database. This database contains records of authorized users and their RFID tags.
5. **Temporary RFID Tag is Given (RFID Module):**
   - For new visitors, a temporary RFID tag is issued. This tag is then used to check the availability in the database.
6. **Alarm Triggered (Alarm Module):**
   - If an unauthorized RFID tag is detected (i.e., the tag is not available in the database), the system triggers an alarm. This indicates a potential security breach, and the gate remains closed.
7. **Gate Remains Closed:**
   - When an unauthorized RFID tag is detected and an alarm is triggered, the gate remains closed to prevent unauthorized access.
8. **Welcome Door Unlocked:**
   - If a valid RFID tag is detected (either from an authorized user or a visitor with a temporary tag), the welcome door is unlocked. This allows access to the campus.
9. **Opens and Closes After 15 Seconds:**
   - Once the welcome door is unlocked, it opens to allow the vehicle to pass and then closes after 15 seconds. This time delay ensures smooth traffic flow and security.
10. **End:**

- This is the final step of the flowchart indicating the end of the process for the current vehicle at the gate. The system is now ready for the next vehicle.

4.3 Modules Description with Algorithms / Pseudo-code

- RFID module
- Micro-controller module
- GSM module
- Gate control module
- Alarm module

4.3.1 RFID Module

An RFID (Radio Frequency Identification) module is an electronic device used for automatic identification and data capture through the use of radio waves.

Components**:**

- RFID Reader:
  - This device emits radio waves to detect and read RFID tags placed in proximity.
  - It captures the unique ID stored on each RFID tag.
- Passive RFID Tags:
  - These tags do not have their own power source. They are powered by the radio waves emitted by the RFID reader.
  - Each tag contains a unique ID that is used for identification.

Functionality:

- Contactless Identification:
  - The RFID reader detects and reads the unique ID from the RFID tag when a vehicle approaches the gate.
  - This allows for contactless identification of the user (student, employee, or visitor).
- Access Control:
  - The unique ID read from the tag is checked against a database of registered IDs to verify if the user is authorized to access the campus.

4.3.2 Micro controller Module

A micro controller module is a compact integrated circuit designed to govern a specific operation in an embedded system. It typically combines a microprocessor, memory, and input/output (I/O) peripherals on a single chip, allowing it to perform real-time control tasks efficiently

Components:

- Micro controller (e.g., Arduino):
    - This is the central processing unit of the system. It controls the overall operation and coordinates between different modules.

Functionality:

- System Control and Processing:
    - The micro controller receives data from the RFID reader and other sensors.
    - It processes this data to determine if the user is authorized.
- Interface Management:
    - The micro controller interfaces with the RFID reader to receive the unique ID.
    - It also interfaces with the GSM modem to send alerts and notifications.
    - It controls the gate mechanics by sending signals to open or close the gate.
    - It triggers the alarm module in case of invalid access attempts.
- Authentication and Gate Control Logic:
    - The micro controller runs the logic to authenticate users based on the unique ID received from the RFID reader.
    - If the ID is valid, it sends a signal to the gate control module to open the gate.
    - If the ID is invalid, it triggers the alarm module.

4.3.3 GSM Module

A GSM (Global System for Mobile Communications) module is a specialized hardware device used to enable communication over the GSM network, allowing devices to send and receive data, SMS (Short Message Service), and voice calls**.**

Components:

- GSM Modem with SIM Card:
    - This module provides cellular connectivity to the system.

Functionality:

- Alerts and Notifications:
    - The GSM modem is used to send alerts and notifications to users (e.g., administrators or security personnel).
    - Alerts can be sent in case of unauthorized access attempts, system malfunctions, or other significant events.

4.3.4 Gate Control Module

A gate control module is an electronic device designed to manage and control the operation of gates or barriers, typically used in access control systems for secure entry and exit points.

Components:

- Gate Access Mechanics:
    - Includes motors, actuators, and other mechanical components responsible for physically opening and closing the gate.

Functionality:

- Physical Gate Operation:
    - Upon receiving a signal from the microcontroller, the gate control module activates the motors and actuators to open the gate.
    - After the vehicle passes through, the gate control module closes the gate after a specified time interval (e.g., 15 seconds).

4.3.5 Alarm Module

An alarm module is an electronic device designed to detect unauthorized access, anomalies, or other predefined conditions and generate an alert through audible, visual, or electronic signals**.**

Components:

- Visual/Audio Indicators:
    - Includes buzzers, sirens, or flashing lights to provide alerts and warnings.

Functionality:

- Alerts and Warnings:

- The alarm module is triggered by the microcontroller in case of events like invalid access attempts.
- It provides visual and/or audio alerts to inform security personnel and deter unauthorized access attempts.

Integration and Workflow.

5. **Vehicle Approaches the Gate:**
   - The RFID reader detects the RFID tag on the vehicle and reads the unique ID.
6. **ID Verification:**
   - The unique ID is sent to the microcontroller, which checks it against the database.
   - If the ID is valid, the microcontroller sends a signal to the gate control module to open the gate.
   - If the ID is invalid, the microcontroller triggers the alarm module.
7. **Gate Operation:**
   - The gate control module opens the gate to allow the vehicle to pass.
   - The gate closes after a specified time interval.
8. **Alerts and Notifications:**
   - If an unauthorized access attempt is detected, the GSM module sends an alert to the relevant authorities.
   - The alarm module provides immediate visual/audio alerts on-site.

5.TESTING

5.1 Test Cases

Test Case ID	Test Case Name/ Objective	Pre requisites/ Pre condition	Test Description/ Testing Process	Expected Result	Actual Result	Status	Action/ Notes
1	Verify valid authorized user access	Authorized user with valid RFID tag	Place RFID tag near the reader and attempt to access the gate	Gate should unlock and open for 15 seconds, then close	Gate unlocked and opened for 15 seconds, then closed	Pass	-
2	Verify invalid RFID tag access	User with invalid RFID tag	Place an invalid RFID tag near the reader and attempt to access the gate	Alarm should trigger and gate should remain closed	Alarm triggered and gate remained closed	Pass	-
3	Verify new visitor access	Visitor without pre-authorization	Issue a temporary RFID tag to the visitor. Place temporary RFID tag near the	Gate should unlock and open for 15 seconds, then close	Gate unlocked and opened for 15 seconds, then closed	Fail	The gate did not open due to some error in RFID tag issued

			reader and attempt to access the gate				
4	Verify new visitor access	Visitor without pre-authorization	Issue a temporary RFID tag to the visitor and Place it near the reader and attempt to access the gate	Gate should unlock and open for 15 seconds, then close	Gate unlocked and opened for 15 seconds, then closed	Pass	-
5	Verify system response to no RFID tag	No RFID tag	Attempt to access the gate without presenting an RFID tag	Gate should remain closed and no action should be taken	Gate remained closed and no action taken	Pass	-
6	Verify system response to unauthorized user	User with RFID tag not registered in the system	Place an unauthorized RFID tag near reader and attempt to access the gate	Alarm should trigger and gate should remain closed	Alarm not triggered	Fail	Alarm module not set properly
7	Verify system response to unauthorized user	User with RFID tag not registered in the system	Place an unauthorized RFID tag near reader and attempt to access the gate	Alarm should trigger and gate should remain closed	Alarm triggered and gate remained closed	Pass	-

8	Verify gate operation timing	Authorized user with valid RFID tag	Place valid RFID tag near the reader and measure the time taken for the gate to open and close	Gate should open within 2 seconds of detecting the RFID tag and close 15 seconds after opening	Gate opened within 2 seconds and closed after 15 seconds	Pass	-
9	Verify GSM module alerts	Any RFID tag (valid or invalid)	Simulate invalid access and check if an alert is sent via the GSM module	Alert/notification should be sent to the predefined contact	Alert/notification sent	Pass	-
10	Verify system under high traffic	Multiple vehicles (up to 1000 entries/exits/hour)	Continuously test system with both RFID tags to ensure it handles high traffic volume without failure	System should handle high traffic volume without failure or significant delay	System handled high traffic volume without failure or significant delay	Pass	-
11	Verify system scalability	Additional gates and users	Integrate additional gates and users into the system and ensure seamless operation	System should support the addition of new gates and users without any performance	System supported the addition of new gates and users without any performanc	Pass	-

				issues	e issues		

6.RESULTS AND CONCLUSION

6.1 Result Analysis

Analyzing the results of a college gate automation system using RFID involves evaluating its performance, efficiency, and impact. Here's a structured approach to performing the analysis:

1. System Overview
   - Purpose: Automating the entry and exit process at college gates.
   - Technology: RFID (Radio Frequency Identification) tags and readers.
   - Components: RFID tags (for students and staff), RFID readers (at gates), database management system, and possibly a user interface.

2. Data Collection
   - Entry/Exit Logs: Data on the number of entries and exits, timestamped.
   - Error Rates: Instances of failed scans or unauthorized access attempts.
   - Operational Data: System uptime, maintenance logs, and technical issues.

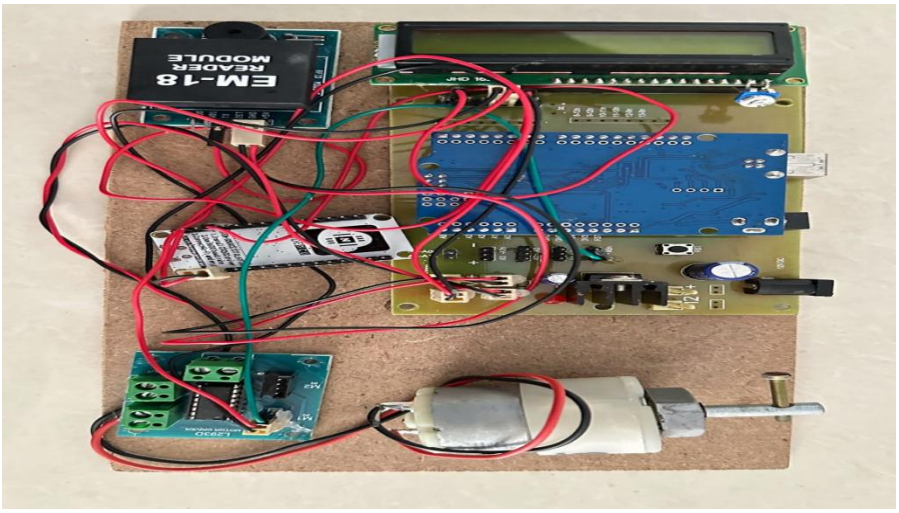
3. Performance Metrics
   - Accuracy: Rate of successful identifications vs. false positives/negatives.
   - Speed: Average time taken for an RFID tag to be read and processed.
   - Reliability: System uptime and downtime statistics.
   - Scalability: Ability to handle peak times without delays or failures.

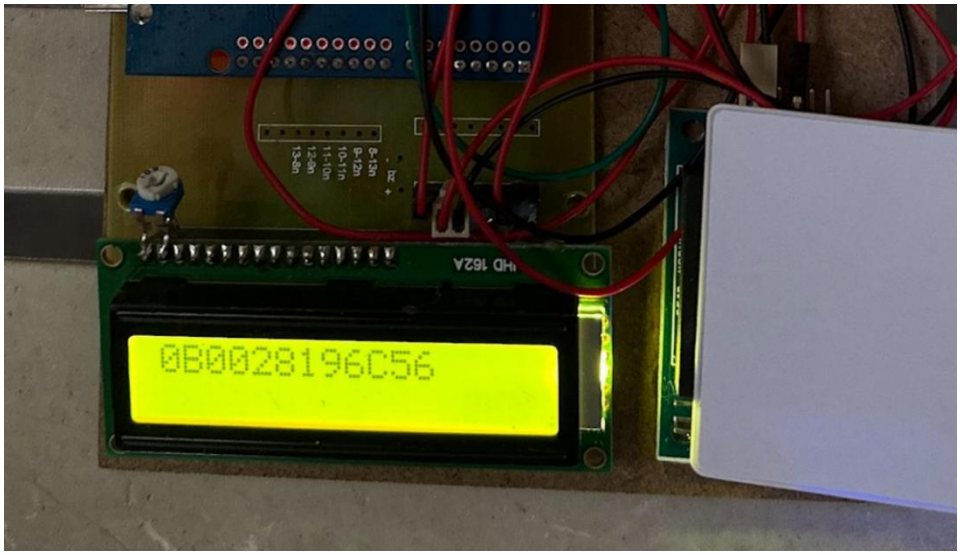
4. Efficiency Analysis
   - Throughput: Number of people processed per minute/hour.
   - Resource Utilization: Usage of computational and human resources.
   - Cost Efficiency: Comparison of operating costs before and after implementation.

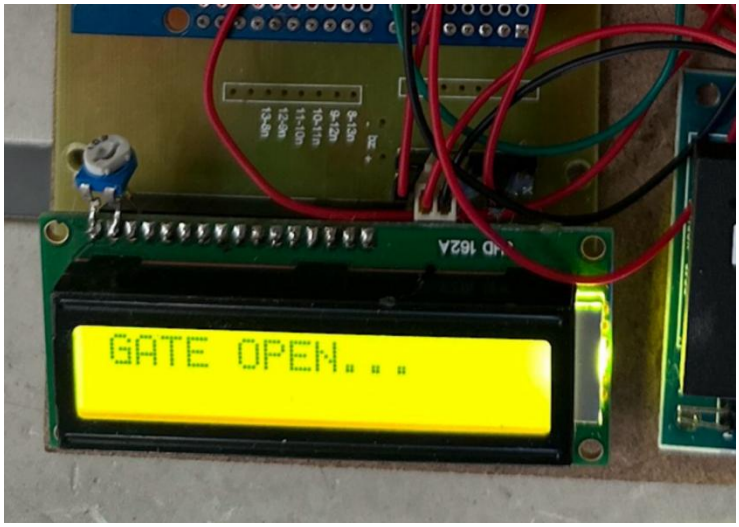
5. Conclusions and Recommendations

- Key Findings: Summarize the main results from the data analysis
- Recommendations:
  - Technical Improvements: Suggestions for hardware or software enhancements.
  - Process Improvements: Changes to operational procedures.
  - Future Research: Areas for further investigation or pilot programs.

By systematically analyzing the data from the RFID based college gate automation system, you can draw meaningful conclusions about its effectiveness and areas for improvement.




0B002819 6C56


GATE OPEN...

6.2 Conclusion & Future Scope

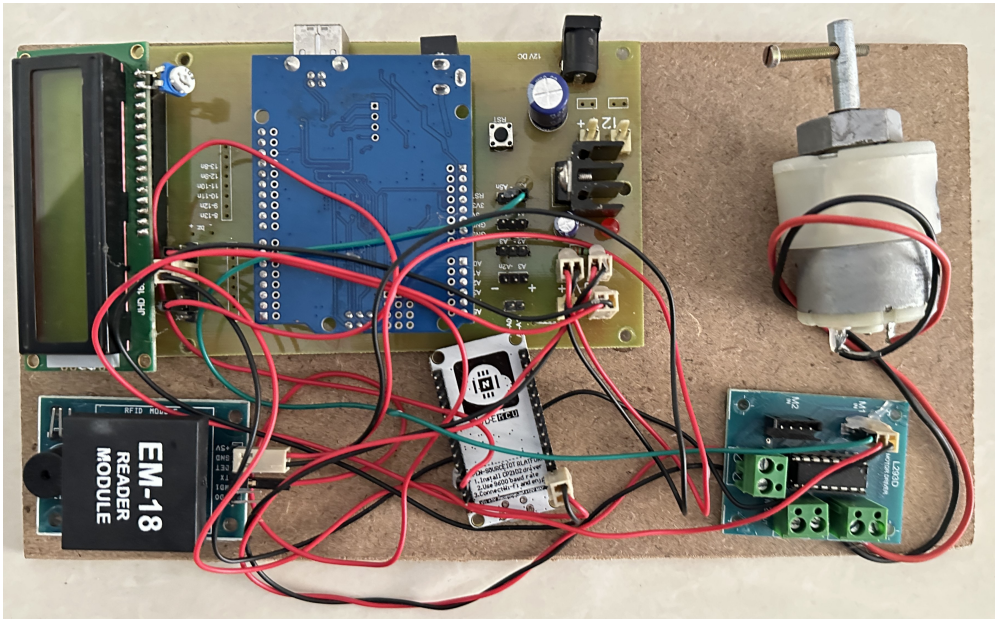
An important development in improving security, effectiveness, and management in educational institutions is the Smart Gate Automation System. The system efficiently automates gate operations, minimizing manual labor and easing traffic congestion by combining RFID technology and Thai ID card identification.

This project uses a centralized database to enhance record-keeping and access control while also making it easier to monitor visitors, staff, and students. By reducing human exposure to inclement weather and operational risks, automated gate barriers enhance safety.

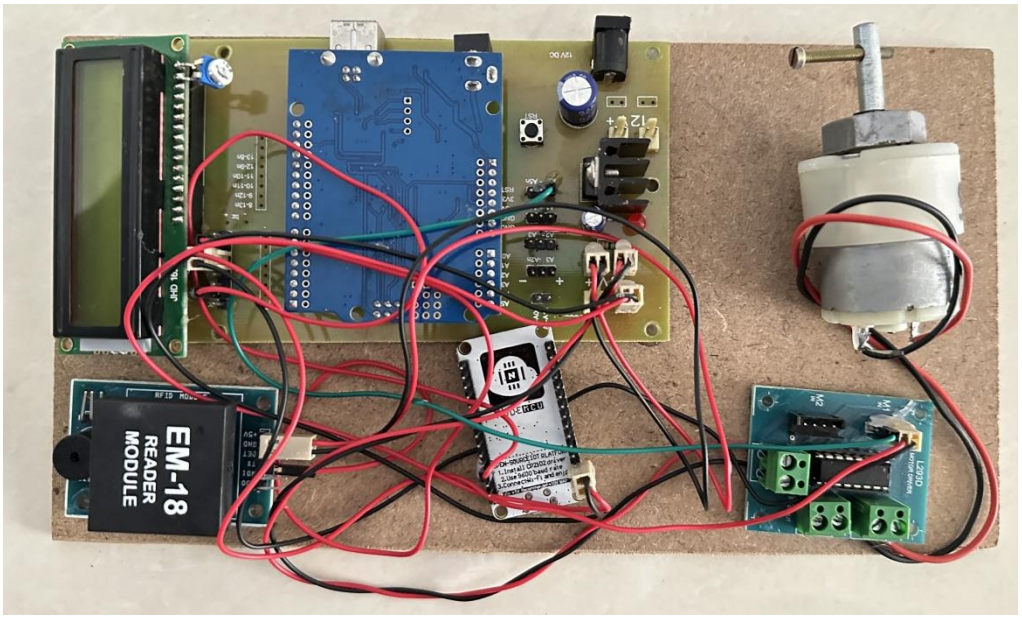
In the future, the technology might find use in locations other than college campuses, providing scalable solutions for metropolitan infrastructure and smart cities. The Smart Gate Automation System is ready to redefine access management standards while contributing to sustainable development thanks to ongoing technological and functional improvements.

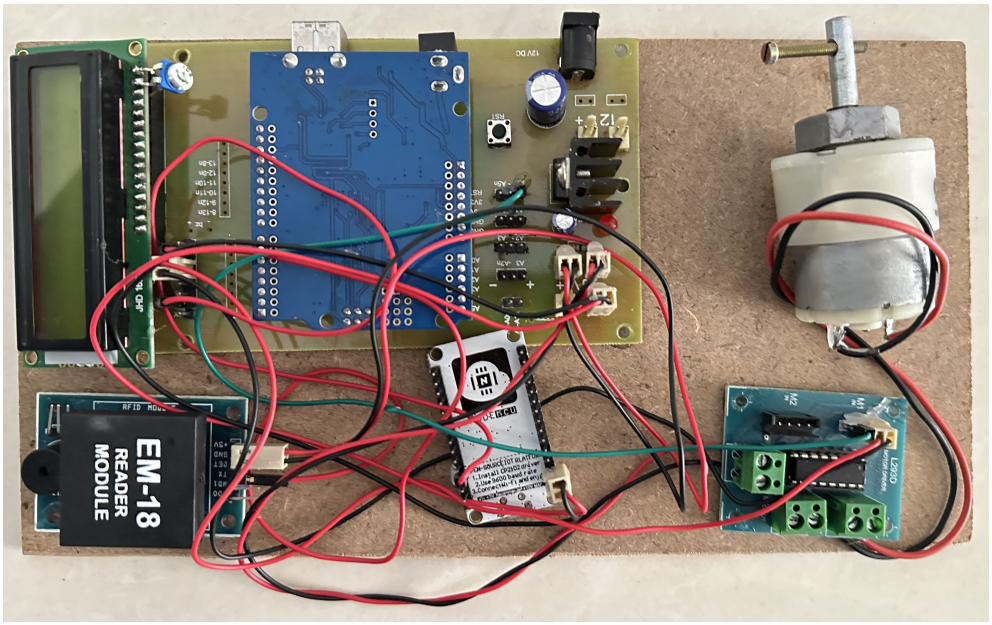
7.APPENDIX

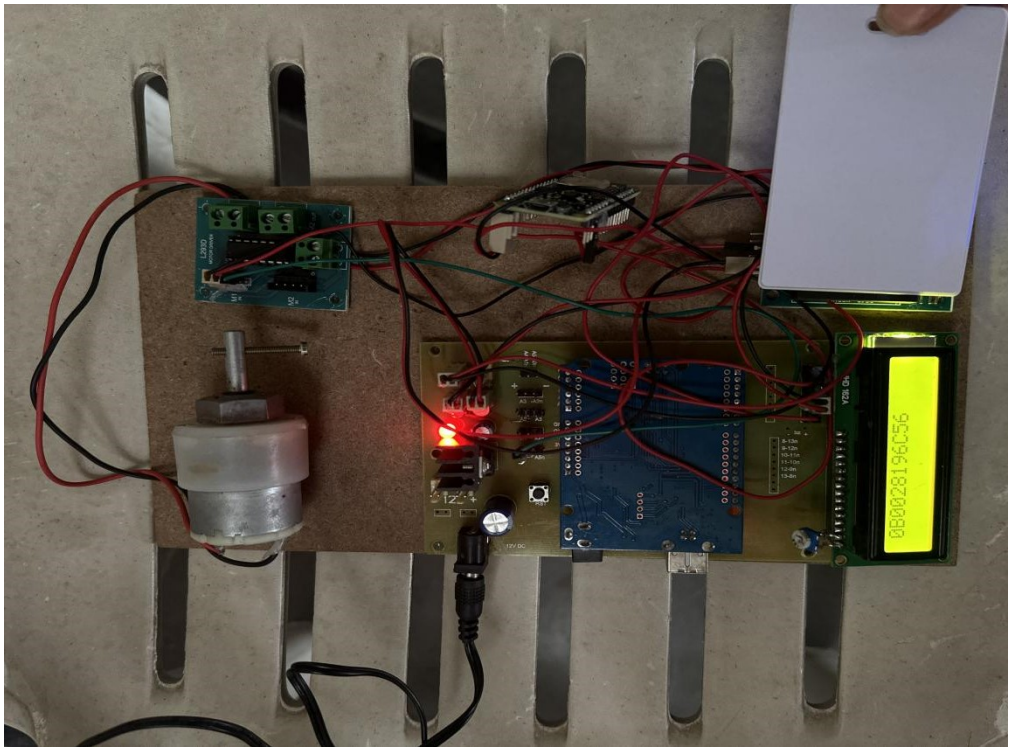
I. Screenshots representing the flow of your project work



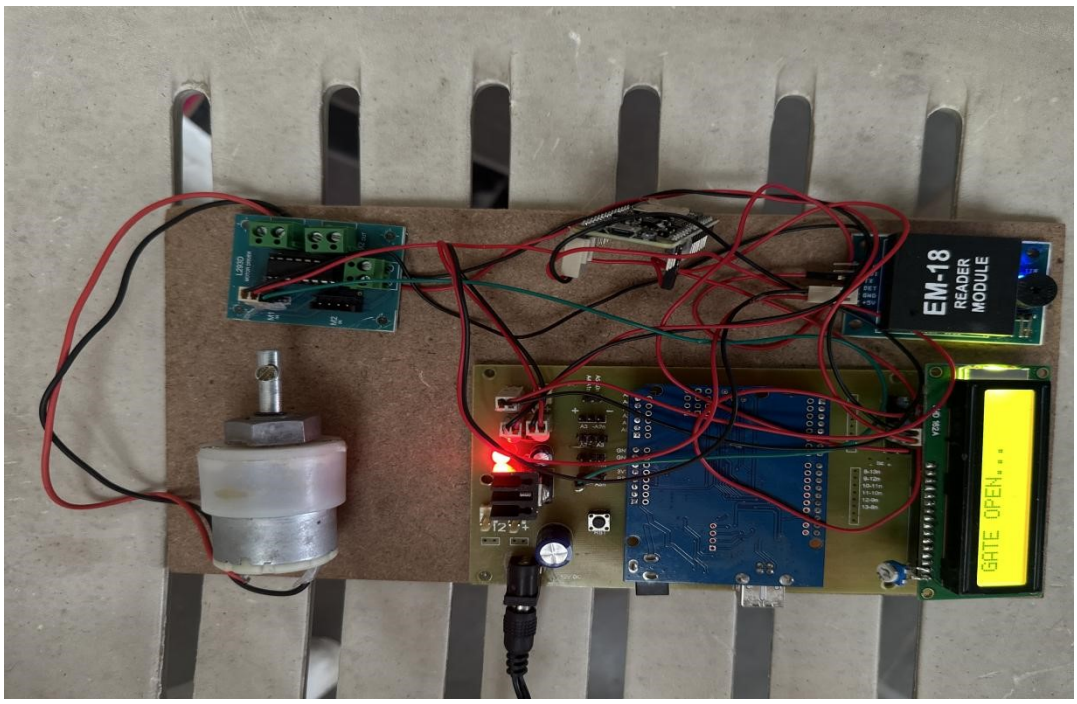
Complete setup of the device



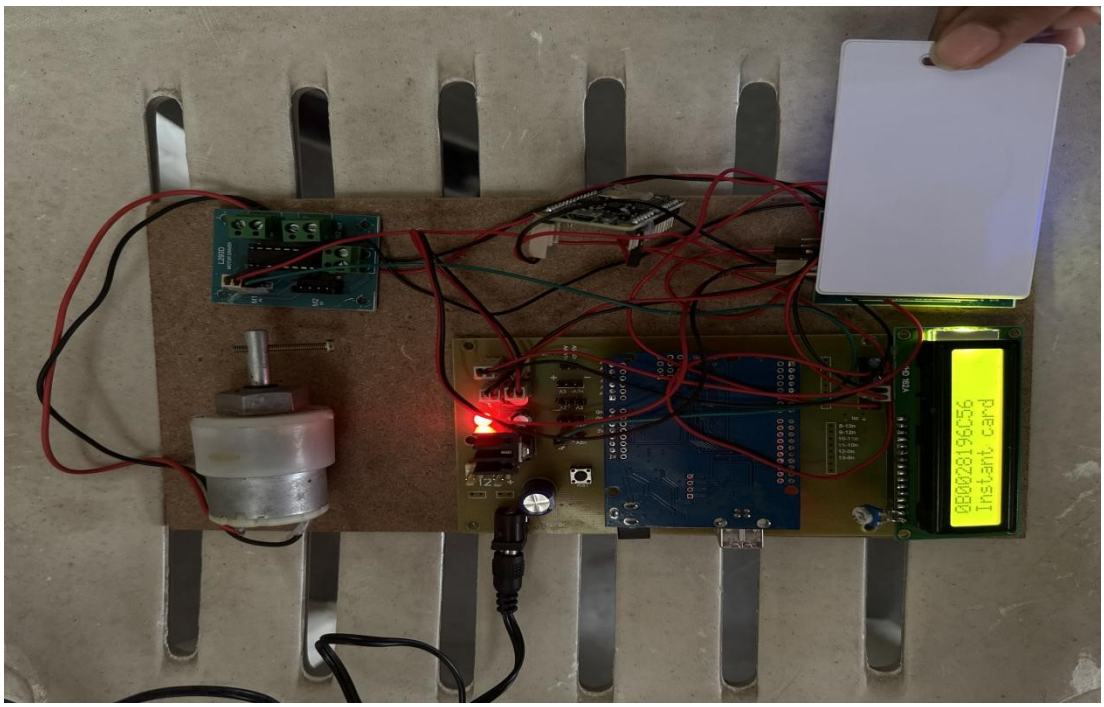




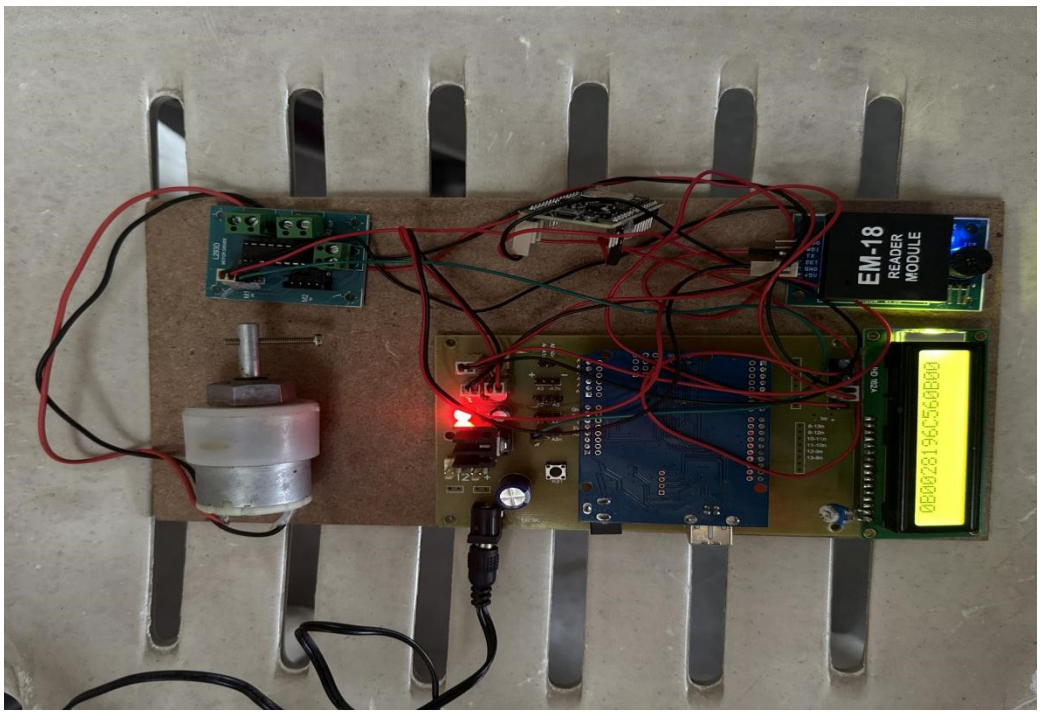
A permanent RFID tag being scanned



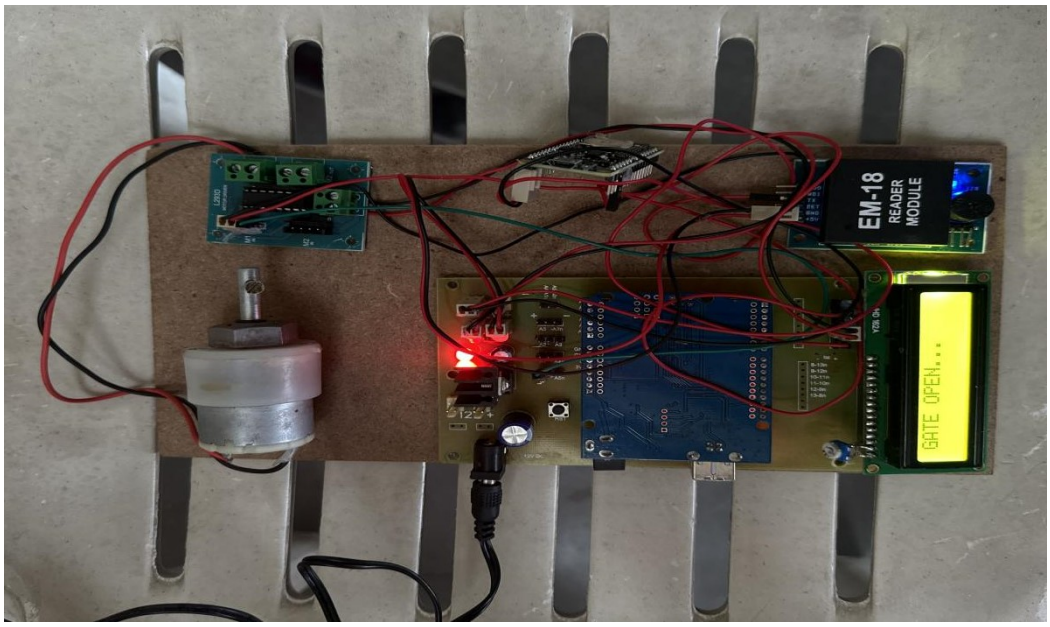
Gate open by successful validation



A Temporary RFID being scanned.



Validating the RFID tag



Gate open on successful validation of instant card.

II. Codes
Code-1:

node_multiwifi.ino

```
#include <WiFiClientSecure.h>   // Include the HTTPS library
#include <ESP8266WiFi.h>        // Include the Wi-Fi library
#include <ESP8266WiFiMulti.h>   // Include the Wi-Fi-Multi library
#include "Arduino.h"
#include <EMailSender.h>
ESP8266WiFiMulti wifiMulti;     // Create an instance of the ESP8266WiFiMulti
class, called 'wifiMulti'
uint8_t connection_state = 0;
uint16_t reconnect_interval = 10000;
WiFiClient  client;
String data1="";
String data2="cmd";
String data=" MESSAGE";
EMailSender emailSend("sainikhitha08@gmail.com", "tvgcjlhvnpdetvvq");
void gmail()
{
 EMailSender::EMailMessage message;

   message.subject = "WEATHER PARAMETER MONI SYSTEM  "+data1;
   message.message = "This_is_Mail_From_ESP8266: "+data1;

   EMailSender::Response resp = emailSend.send("sainikhitha08@gmail.com",
message);

   Serial.println("Sending status: ");

   Serial.println(resp.status);
```

```
   Serial.println(resp.code);
   Serial.println(resp.desc);
}
void upload()
{
const char* server4 = "api.thingspeak.com";
const char* _getLink4 =
"https://api.thingspeak.com/update?api_key=91SHW5GUCCRO6Y5M&field1="; //
Thingspeak.com
//const char* _getLink4 =
"https://api.thingspeak.com/update?api_key=EMSXF1FT72GGQN9X&field1="; //
Thingspeak.com

 // Serial.println("data uploading");delay(1000);
  client.connect(server4,80);
 if (client.connect(server4,80))     // "184.106.153.149" or api.thingspeak.com
https://api.thingspeak.com/apps/thinghttp/send_request?api_key=CT9B331KB5PLM
1G5
  {
   String getStr4 = _getLink4;
   client.print("GET "+getStr4+data1+"\n");
   client.print("HTTP/1.1\n");
   client.print("Host: api.thingspeak.com\n");
   client.print("Connection: close\n\n\n");
  }
  client.stop();

}

void readdata()
{
  data1="";delay(1000);
const char* server4 = "api.thingspeak.com";
```

```
const char* _getLink4 = "
https://api.thingspeak.com/channels/562742/fields/1/last.txt"; // Thingspeak.com


  //Serial.println("data uploading");delay(1000);
  client.connect(server4,80);
 if (client.connect(server4,80))     // "184.106.153.149" or api.thingspeak.com
https://api.thingspeak.com/apps/thinghttp/send_request?api_key=CT9B331KB5PLM
1G5
  {
    String getStr4 = _getLink4;
    client.print("GET "+getStr4+"\n");
    client.print("HTTP/1.1\n");
    client.print("Host: api.thingspeak.com\n");
    client.print("Connection: close\n\n\n");
    client.available();
    data1=client.readString();delay(1000);
    //Serial.println(data1);delay(1000);

if(data1[0]=='*')
{
  if(data2==data1)
  {


  }
  else
  {
  Serial.println(data1);upload();
  }
  data2=data1;
}
/*
```

```
if((data1=="light1on")||(data1=="light1off")||(data1=="light2on")||(data1=="light2off")
||(data1=="fan1on")||(data1=="fan1off")||(data1=="fan2on")||(data1=="fan2off"))
{
  Serial.print(data1);delay(1000);upload();
}

    if(data1[0]=='*')
    {
   Serial.println(data1);delay(10000);upload();
    }
    if((data1=="1")||(data1=="2")||(data1=="3")||(data1=="4")||(data1=="0"))
    {
   Serial.print(data1);delay(10000);
      }
      */
  }
  client.stop();
}


void setup()
{
  Serial.begin(9600);         // Start the Serial communication to send messages to the
computer
  delay(10);
  //Serial.println('\n');

 // add Wi-Fi networks you want to connect to
  wifiMulti.addAP("ZTE-sUQdqa", "5hjgxyh9");
  wifiMulti.addAP("project", "project.123");
  wifiMulti.addAP("123456789", "123456789");

  //Serial.println("Connecting ...");
  int i = 0;
```

```
  while (wifiMulti.run() != WL_CONNECTED) { // Wait for the Wi-Fi to connect:
scan for Wi-Fi networks, and connect to the strongest of the networks above
    delay(250);
    //Serial.print('.');
  }
  //Serial.println('\n');
  //Serial.print("Connected to ");
  //Serial.println(WiFi.SSID());              // Tell us what network we're connected to
  //Serial.print("IP address:\t");
 Serial.println(WiFi.localIP());           // Send the IP address of the ESP8266 to the
computer
  //Serial.println('\n');

  //readdata();
//gmail();
}


void loop()
{
while(1)
{
//readdata();

 while(Serial.available())
 {
  data1=Serial.readString();delay(1000);
  upload();
  gmail();

 }

}
}
```

Code-2:

Rfid_based_gate_control.io

```
#include <SoftwareSerial.h>
const byte rxPin = 6;
const byte txPin = 7;
SoftwareSerial rfid (rxPin, txPin);
#include <LiquidCrystal.h>
const int rs = 13, en =12, d4 = 11, d5 = 10, d6 = 9, d7 = 8;
LiquidCrystal lcd(rs, en, d4, d5, d6, d7);
int temp=0;
String iot="";
int m1=5;
int m2=4;
void setup()
{
  pinMode(m1,OUTPUT);  pinMode(m2,OUTPUT);
  digitalWrite(m1,LOW);digitalWrite(m2,LOW);
 lcd.begin(16, 2);lcd.print("hello, world!");
 rfid.begin(9600);delay(1000);
 Serial.begin(9600);
 lcd.clear();lcd.print("Ready to use >>>");
}

void loop()
{
while(rfid.available())
{
  String card=rfid.readString();
  lcd.clear();lcd.print(card);delay(1000);
  iot="CARD_NUMBER_"+card;delay(1000);
  Serial.println(iot);delay(1000);
```

```
  if(card=="5500122BA3CF")
  {
  lcd.setCursor(0,1);lcd.print("Valid card");delay(1000);
   lcd.clear();lcd.print("GATE OPEN...");
   digitalWrite(m1,HIGH);digitalWrite(m2,LOW);delay(2000);
digitalWrite(m1,LOW);digitalWrite(m2,LOW);delay(3000);
   digitalWrite(m1,LOW);digitalWrite(m2,HIGH);delay(2000);
digitalWrite(m1,LOW);digitalWrite(m2,LOW);delay(3000);
   lcd.clear();lcd.print("Ready to use >>>");
  }
  else if(card=="550012E7C868")
  {
  lcd.setCursor(0,1);lcd.print("Valid card");delay(1000);
   lcd.clear();lcd.print("GATE OPEN...");
  digitalWrite(m1,HIGH);digitalWrite(m2,LOW);delay(2000);
digitalWrite(m1,LOW);digitalWrite(m2,LOW);delay(3000);
   digitalWrite(m1,LOW);digitalWrite(m2,HIGH);delay(2000);
digitalWrite(m1,LOW);digitalWrite(m2,LOW);delay(3000);
   lcd.clear();lcd.print("Ready to use >>>");
  }
  else
  {
  lcd.setCursor(0,1);lcd.print("Instant card");delay(1000);
  temp=temp+1;delay(1000);
  if(temp==1)
  {
  lcd.clear();lcd.print("GATE OPEN...");
  digitalWrite(m1,HIGH);digitalWrite(m2,LOW);delay(2000);
digitalWrite(m1,LOW);digitalWrite(m2,LOW);delay(3000);
   digitalWrite(m1,LOW);digitalWrite(m2,HIGH);delay(2000);
digitalWrite(m1,LOW);digitalWrite(m2,LOW);delay(3000);
   lcd.clear();lcd.print("Ready to use >>>");
  }
  else
```

```
  {
  lcd.clear();lcd.print("NOT ALLOWED");

  lcd.setCursor(0,1);lcd.print("TRY AGAIN");delay(2000);
  lcd.clear();lcd.print("Ready to use >>>");
  }
  }
}
}
```

III. References

1.K. Ahsan, H. Shah, and P. Kingston, “RFID Applications: An Introductory and Exploratory Study,” IJCSI Int. J. Comput. Sci. Issues, vol. 7, no. 1, pp. 1–7, 2019.

2. S. Guennouni, A. Ahaitouf, and A. Mansouri, “Multiple object detection using OpenCV on an embedded platform,” Colloq. Inf. Sci. Technol. Cist, vol. 2015–January, no. January, pp. 374–377,2018

3.Juels A. 2006. RFID security and privacy: A research survey. IEEE journal on selected areas in communications. 24(2): 381-394.

4. Nath S., Banerjee P., Biswas R. N., Mitra S. K. & Naskar M. K. 2016, December. Arduino based door unlocking system with real time control. In Contemporary Computing and Informatics (IC3I) 2016 2nd International Conference on (pp. 358-362). IEEE.

5. Goodrum P. M., McLaren M. A. & Durfee A. 2016. The application of active radio frequency identification technology for tool tracking on construction job sites. Automation in Construction.

6. Saifuddin Mahmud, Ishtiaq Reza Emon, Md. Mohaimin Billah, “Automated Gate Controlling System,” IJCTT - volume 27, No.1, 2015

7. Arunjyothi, B., and B. Harikrishna. "Automated Railway Gate Control Using Internet of Things," Soft Computing: Theories Applications: Proceedings of SoCTA, Springer Singapore, 2020.

8. Wang, Shan, Ranjeet Yadav, R. Raffik, Jyoti Bhola, Manik Rakhra, Julian L. Webber, and Abolfazl Mehbodniya. "Wireless Sensor Network