MAJOR PROJECT-1

FINAL REPORT

For

"TrackNClassify: Enhanced Security System for Visitors Authentication"

Submitted By:

Specialization	SAP ID	Name
CCVT B6 N(H)	500095936	Siddharth Kirti Gautam
CCVT B1 Hons.	500091948	Aditi Negi
CCVT B1 Hons.	500091576	Steve S. Yadav

Department of Systemics
School of Computer Science
UNIVERSITY OF PETROLEUM & ENERGY STUDIES,
DEHRADUN- 248007, Uttarakhand

Project Mentor
Dr. Shresth Gupta

Project Evaluator
Mr. SK Tausif Rahman

DECLARATION

We, **Team Tracify** (Siddharth Kirti Gautam, Aditi Negi, Steve S. Yadav) hereby declare that the work presented in this project report entitled **"TrackNClassify"** in partial fulfilment of the requirement for the Award/Certificate for the completion of Major Project-1 from UPES, Dehradun, Uttarakhand. This report is an authentic record of our work carried out during our 7th Semester for Major Project-1 at School of Computer Science Dehradun, Uttarakhand, under the guidance of **Dr. Shresth Gupta**, ONGC Dehradun, Uttarakhand.

Signature of the Students:

(Siddharth Kirti Gautam)

(Aditi Negi)

steve yadav

(Steve S. Yadav)

CERTIFICATE OF ACCEPTANCE

This is to certify that **Mr. Siddharth Kirti Gautam, Ms. Aditi Negi, Mr. Steve S. Yadav** students of B.Tech. CSE (spec. CCVT) of UPES, Dehradun, Uttarakhand has submitted their work for Major Project-1 at School of Computer Science, UPES, Dehradun, Uttarakhand.

The project work entitled "TrackNClassify: Enhanced Security System for Visitor Authentication" embodies the original work done by all the team mates of Team Tracify during their 7th Semester.

Signature of Project Guide

Dr. Shresth Gupta

Signature of Evaluator

22/11.

ACKNOWLEDGEMENT

We, **Team Tracify** (Siddharth Kirti Gautam, Aditi Negi, Steve S. Yadav), would like to express our heartfelt gratitude to **School of Computer Science, UPES, Dehradun** for providing us with this incredible opportunity to work on our project, "TrackNClassify," as part of Major Project-1 during our 7th semester.

We extend our sincere thanks to **Dr. Shresth Gupta** for his invaluable guidance, support, and encouragement throughout the completion of this project. His expertise and mentorship played a crucial role in the successful execution of our work.

We also wish to thank the **Department of Systemics** at UPES, Dehradun, for their cooperation and support, which greatly contributed to the practical aspects of this project.

Lastly, we express our deep gratitude to our families and friends for their unwavering support, motivation, and encouragement throughout this journey.

Table of Content:

1. Project Title

TrackNClassify - Enhanced Security System for Visitor Authentication

2. Abstract

The Enhanced Security System for Employee and Visitor Authentication is being developed to address growing concerns around security in organizations. The system will combine image recognition (face recognition), QR code scanning, and RFID technology to provide a multilayered, efficient, and user-friendly solution for authenticating individuals entering or exiting premises. By integrating modern technologies like biometric sensors, smart cards, and mobile applications, the system will ensure real-time monitoring, logging, and security breach detection. Built using the MERN stack (MongoDB, Express.js, React, and Node.js), it aims to streamline management while offering robust security.

3. Introduction

In the modern world, ensuring security in both private and public sectors has become a top priority due to increasing threats and the need for stringent access control. Traditional security measures, such as manual logbooks, keycards, or simple ID systems, are no longer sufficient to prevent unauthorized access and security breaches. These systems often suffer from vulnerabilities like forgery, manipulation, and inefficiency, especially in environments where a large number of individuals are entering and exiting on a regular basis.

The **Enhanced Security System for Employee and Visitor Authentication** aims to address these challenges by offering **a multifaceted authentication** solution that leverages the latest technologies - **image recognition, QR code scanning,** and **RFID** systems. By combining these three powerful authentication mechanisms, we aim to create a robust, scalable, and real-time system that provides comprehensive security coverage for organizations.

The system is designed to streamline access control, ensuring that only authorized individuals are allowed entry, while simultaneously keeping a detailed and up-to-date record of their activities on the premises.

The use of **biometric face recognition** makes it difficult for unauthorized individuals to bypass security, as this technology provides a high level of accuracy and precision. Additionally, **RFID technology** allows

for fast and efficient entry of employees and visitors using RFID cards, while **QR code scanning** facilitates temporary access for visitors, eliminating the need for physical cards. This security solution is being built using the **MERN stack** (MongoDB, Express.js, React, and Node.js), a popular framework that allows for efficient real-time data processing and a seamless user experience. The **React-based front-end** provides a user-friendly interface for security personnel to monitor activities, while the back-end handles complex processes such as real-time data synchronization, authentication, and logging.

By integrating these cutting-edge technologies into a single platform, we aim to develop a security system that not only protects the premises but also enhances the overall efficiency of the authentication process. The project focuses on achieving real-time monitoring and logging, immediate detection of security breaches, and easy management of all data through a comprehensive dashboard interface.

4. Problem Statement

The current authentication systems in many organizations rely on single-layer methods such as ID cards or manual logbooks, which are susceptible to fraud, forgery, and inefficiency. These systems lack real-time monitoring, which delays response times to potential security breaches. There is a growing need for a system that can combine multiple authentication methods to ensure comprehensive security, while also providing a user-friendly interface for managing and monitoring real-time data.

5. Literature Review

Security systems have evolved significantly over the past few decades, particularly in the realm of authentication technologies. Traditional security systems relied heavily on single-point authentication mechanisms like ID badges, PIN codes, and manual logbooks. However, these systems have shown their limitations in terms of security, scalability, and efficiency. The introduction of advanced technologies such as biometrics, RFID, and QR code-based systems has revolutionized how we think about access control and security.

Suethanuwong and Sukkasame (2023) explore an integrated access control system that combines RFID with face verification and QR code-based enrollment. The system enhances security by requiring multiple layers of authentication, ensuring that both the RFID tag and the facial biometric features match before granting access. This approach addresses the limitations of traditional RFID systems, which can be vulnerable to spoofing or stolen tags. The use of QR codes for enrollment further simplifies user management, making it more convenient for users to register their credentials through a quick and secure process. This study provides a valuable framework for combining multiple technologies to enhance security in access control systems [1].

Vandana and Kaur (2021) focus on the role of biometric systems in identification and verification. Their study discusses the importance of biometric features, such as fingerprints, iris, and facial recognition, as reliable methods for securing access control systems. They highlight the growing trend of adopting biometrics in both public and private sectors due to their high accuracy in identifying individuals. However, the study also addresses challenges such as privacy concerns, data storage issues, and the need for robust systems that can handle large-scale deployments efficiently. The authors stress the importance of combining biometric systems with other technologies, such as RFID, to enhance overall security [2].

Selvaraj et al. (2021) present a practical application of automatic door control using a Raspberry Pi. In this system, RFID tags are used to identify authorized individuals, while the Raspberry Pi acts as the controller that manages access to the door. The study shows how low-cost and accessible hardware can be effectively utilized in access control systems, especially in small-scale or personal projects. The Raspberry Pi-based system demonstrates how such technologies can be integrated into larger IoT frameworks, providing scalability and flexibility for users. While the system is effective in controlling access, it lacks biometric verification, which could be added for enhanced security [3].

Leyu et al. (2021) propose an RFID access control system that leverages multiple biometric features, such as face and fingerprint recognition, to secure restricted areas. Their study focuses on the design and implementation of this system, with an emphasis on using biometric data to enhance the security of RFID-based systems. By incorporating multiple biometric identifiers, the system can better distinguish between authorized and unauthorized users, reducing the likelihood of access being granted based solely on an RFID tag. The study demonstrates that integrating multiple biometric features improves accuracy, reduces false positives, and enhances security in sensitive environments [4].

The Use of QR Codes in Security Systems (2021) explores the use of QR codes as an alternative or complementary method for securing access control systems. The study highlights how QR codes can provide a flexible and cost-effective way of identifying users, especially in environments where physical cards or tags are impractical. The authors discuss how QR codes can be dynamically generated and scanned for authentication purposes, offering a high level of convenience and security. However, the study also notes potential vulnerabilities, such as QR code spoofing, which necessitates the integration of other security measures, like biometrics or encryption, to ensure system integrity [5].

6. Objectives

The main objectives of this project are:

- **Multifaceted Authentication**: Develop a system that integrates image recognition, QR codes, and RFID technology to authenticate individuals.
- **Database Integration**: Ensure seamless integration with MongoDB to store logs and manage user data.
- **Real-time Data Processing**: Implement real-time data processing for immediate detection of unauthorized access.
- **User-friendly Interface**: Develop a React-based interface for easy management and monitoring by security personnel.
- **Comprehensive Logging**: Maintain detailed logs to track entry and exit times, as well as detect and prevent potential security breaches.

7. Methodology

The development process for this project follows the following phases:

1. **Requirement Gathering**: Identifying the hardware components and software tools required for the system, such as biometric sensors for face recognition, RFID readers, and mobile devices for QR code scanning.

2. **System Design**: Designing a full-stack architecture using the MERN stack to handle both the front-end (React) and back-end (Node.js, Express.js, MongoDB).

3. **Implementation**:

- QR Code Scanning: Enabling QR code generation and scanning for visitor passes.

- RFID Integration: Using RFID readers to capture employee and visitor data, linking it to stored information.

- Node-Mailer Integration: Using Node install the dependencies for proper functioning of the application.

4. **Database Setup**: Setting up MongoDB to store authentication logs, user details, and movement history.

5. **Front-end Development**: Building a React-based interface for security personnel to easily monitor and manage the system.

6. **Testing and Validation**: Conducting unit tests for each module, followed by integration tests to ensure the system works as expected.

7. **Deployment and Monitoring**: Deploying the system on a cloud platform and ensuring real-time data synchronization across all components.

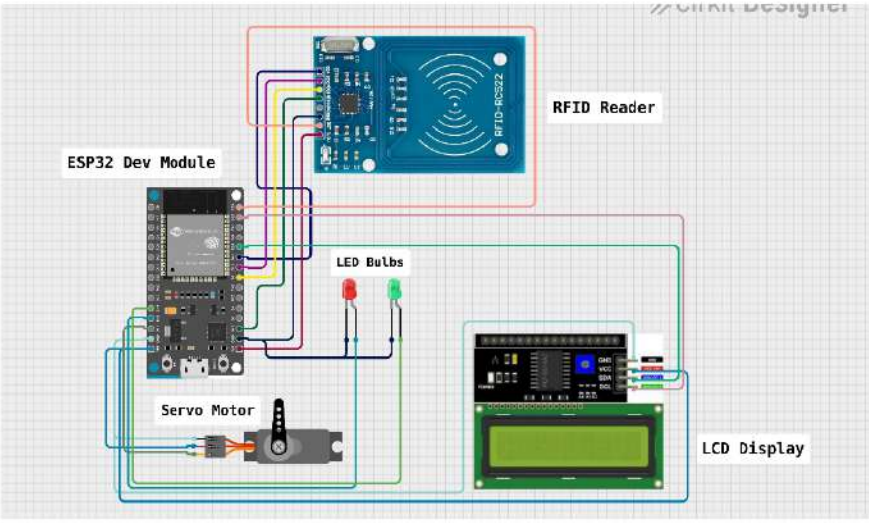
8. System Requirements

Software:

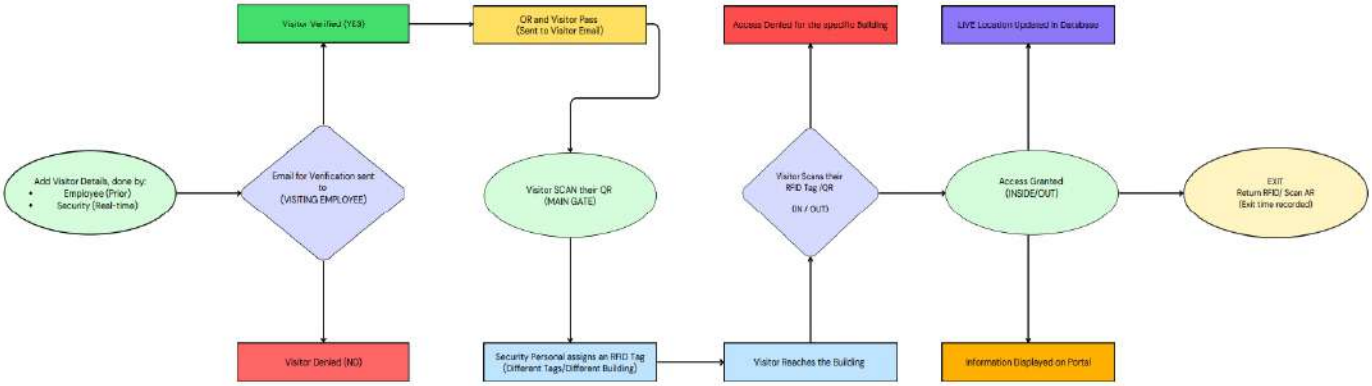
- **MongoDB**: Database management for logs and user data.
- **Express.js**: Backend framework to manage server-side functionality.
- **React**: Front-end library for user interface development.
- **Node.js**: JavaScript runtime for building the back end.
- **JavaScript (JS)**: Programming language for both front-end and back-end development.
- **CSS**: Styling language for the user interface.
- **Arduino IDE**: For coding the microcontroller.

Hardware:

- **RFID Reader**: For scanning RFID tags.
- **Server**: Laptop/PC
- **ESP32 Microcontroller** (for integrating hardware components with our server & database)
- **Cameras**: For QR Code Reading.
- **RFID tags**: To link Visitors data with tags.



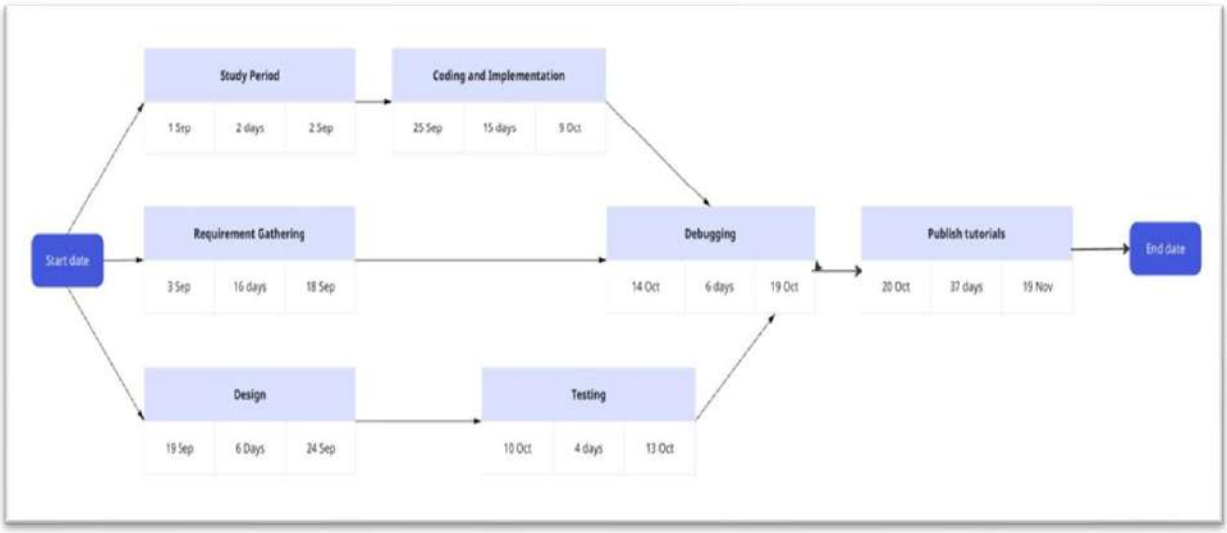
Architecture Diagram



Flow Chart

9. PERT Chart

A PERT (Program Evaluation Review Technique) chart will be used to visualize and manage the project's timeline and critical path. The key activities are as follows:



10. Results

Visualization of Software Implementation:

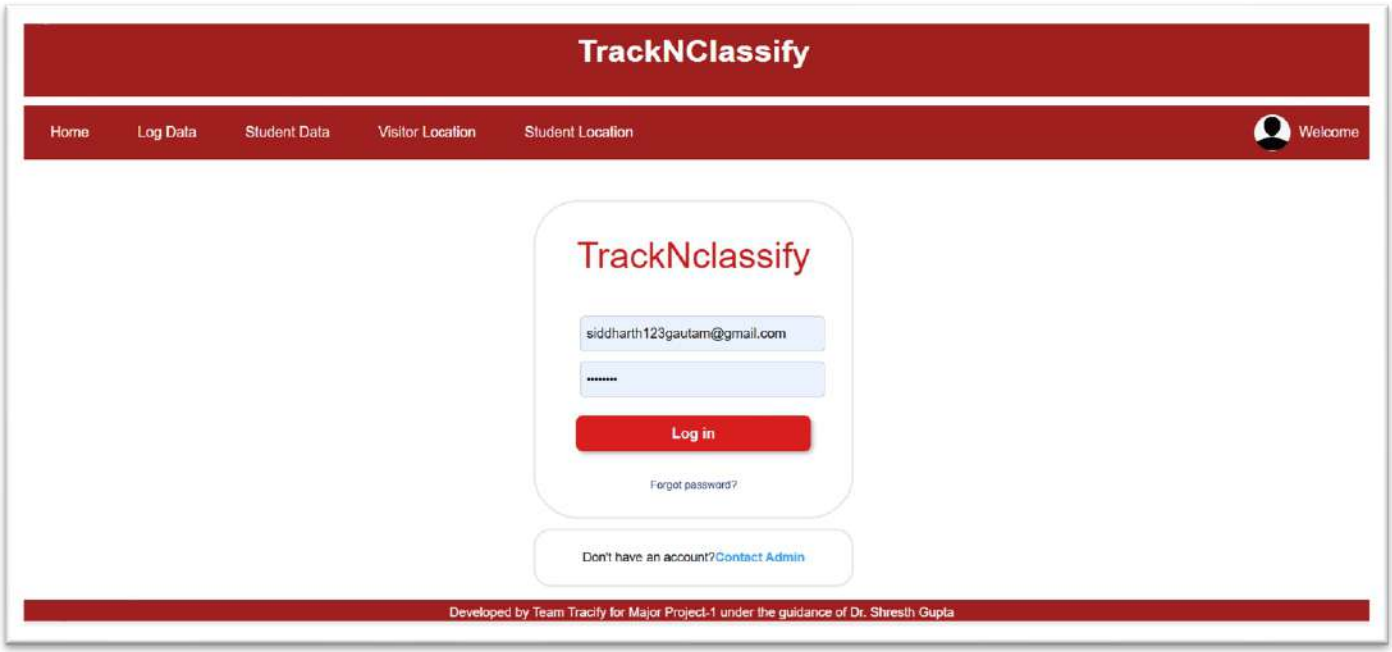


Fig: Login Page

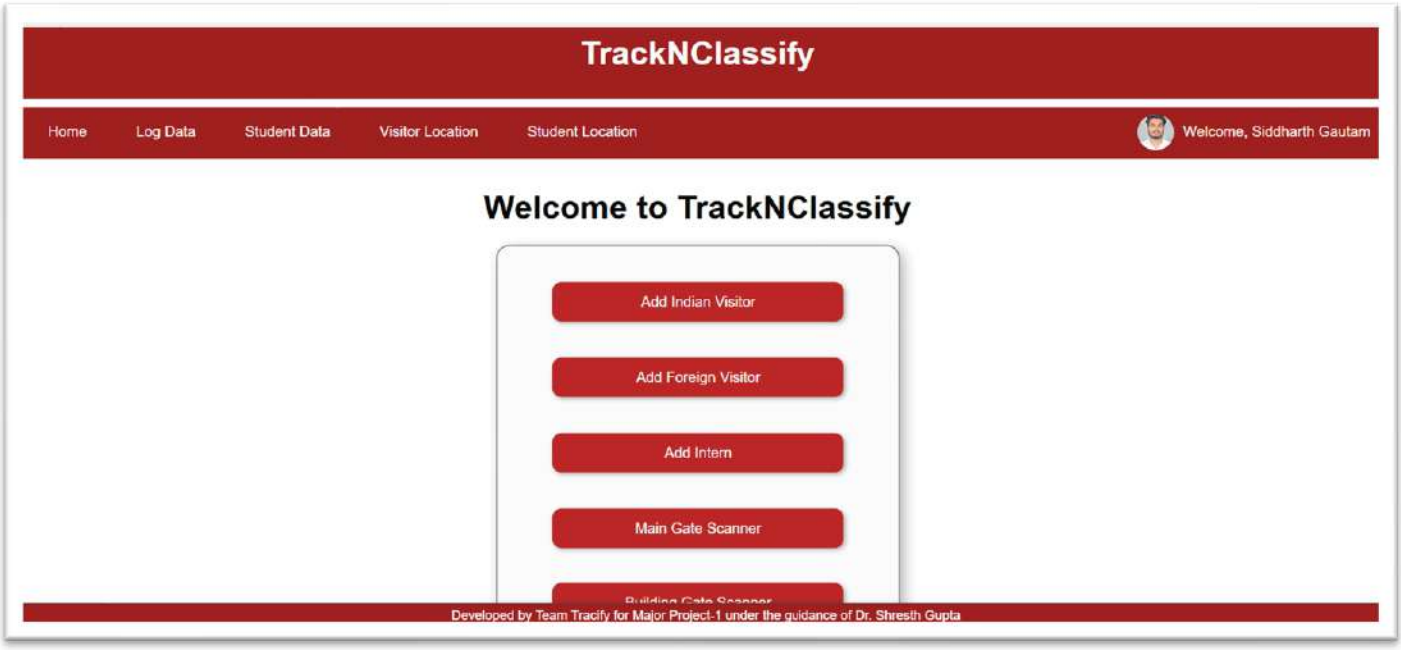


Fig: Home Page

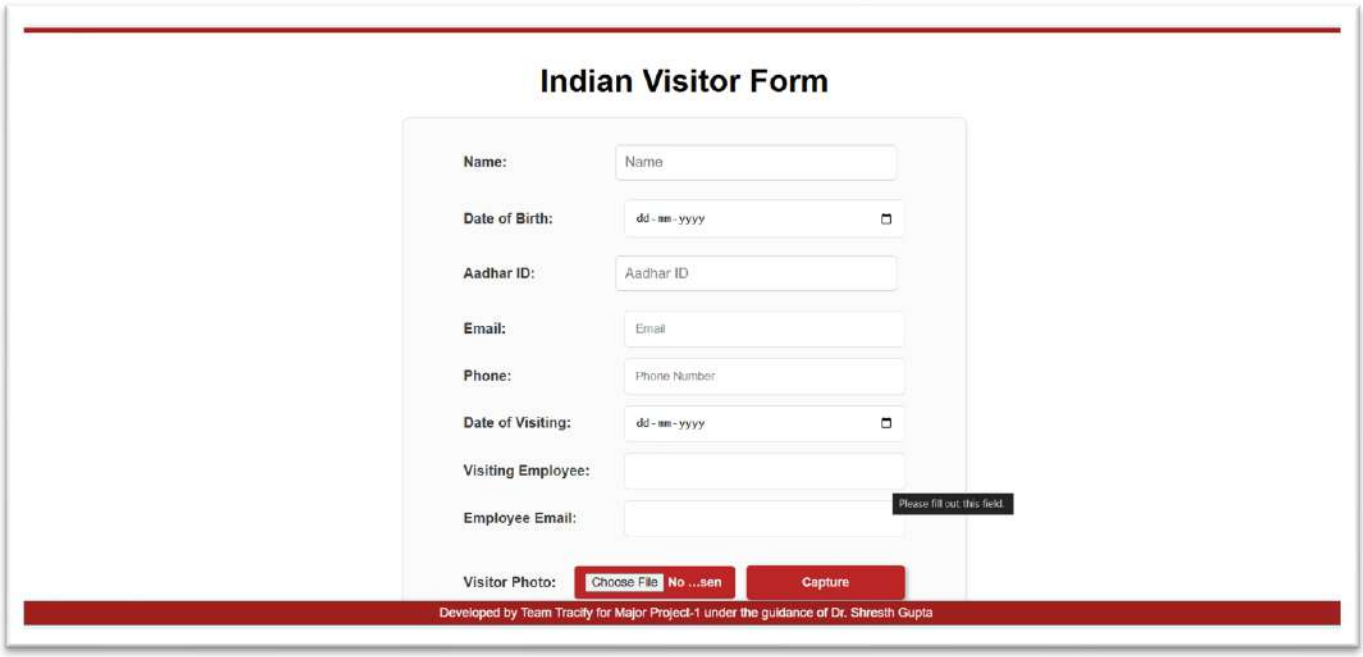


Fig: Adding an Indian Visitor

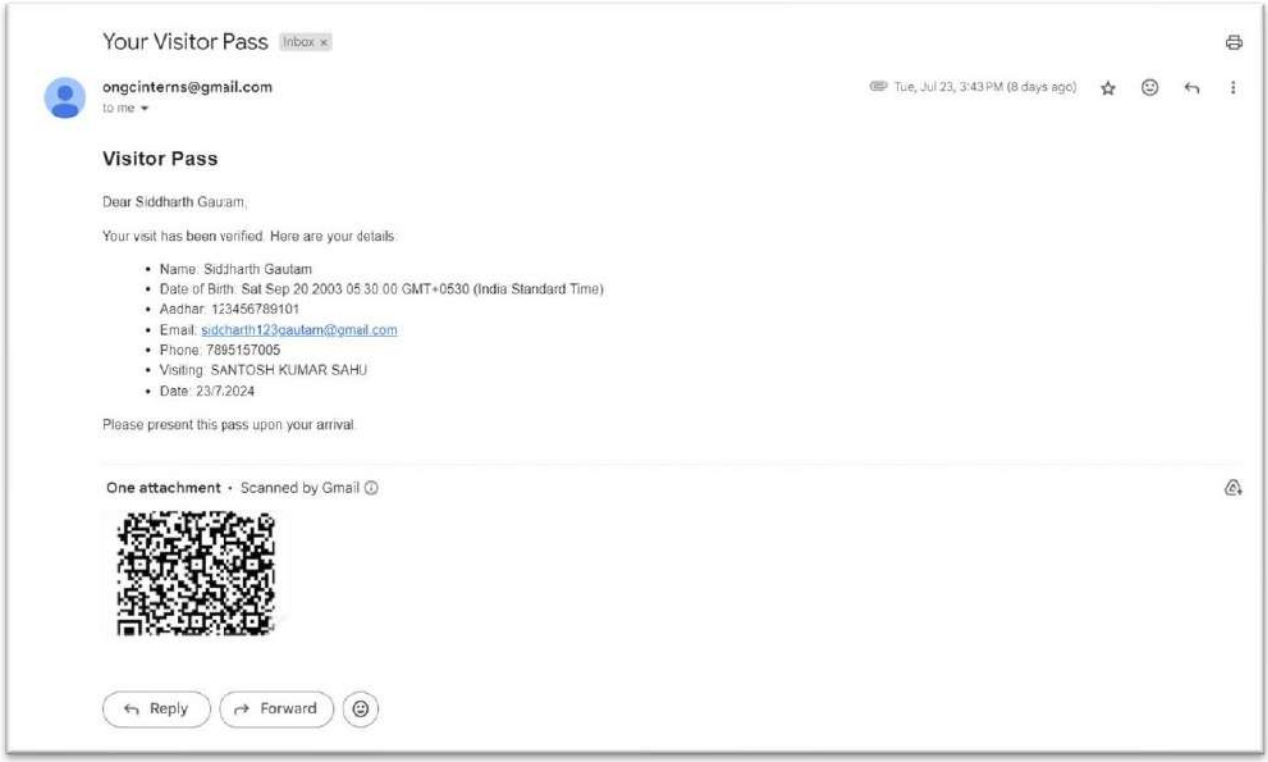


Fig: Mail Received by the Visitor After Being Authenticated (QR)

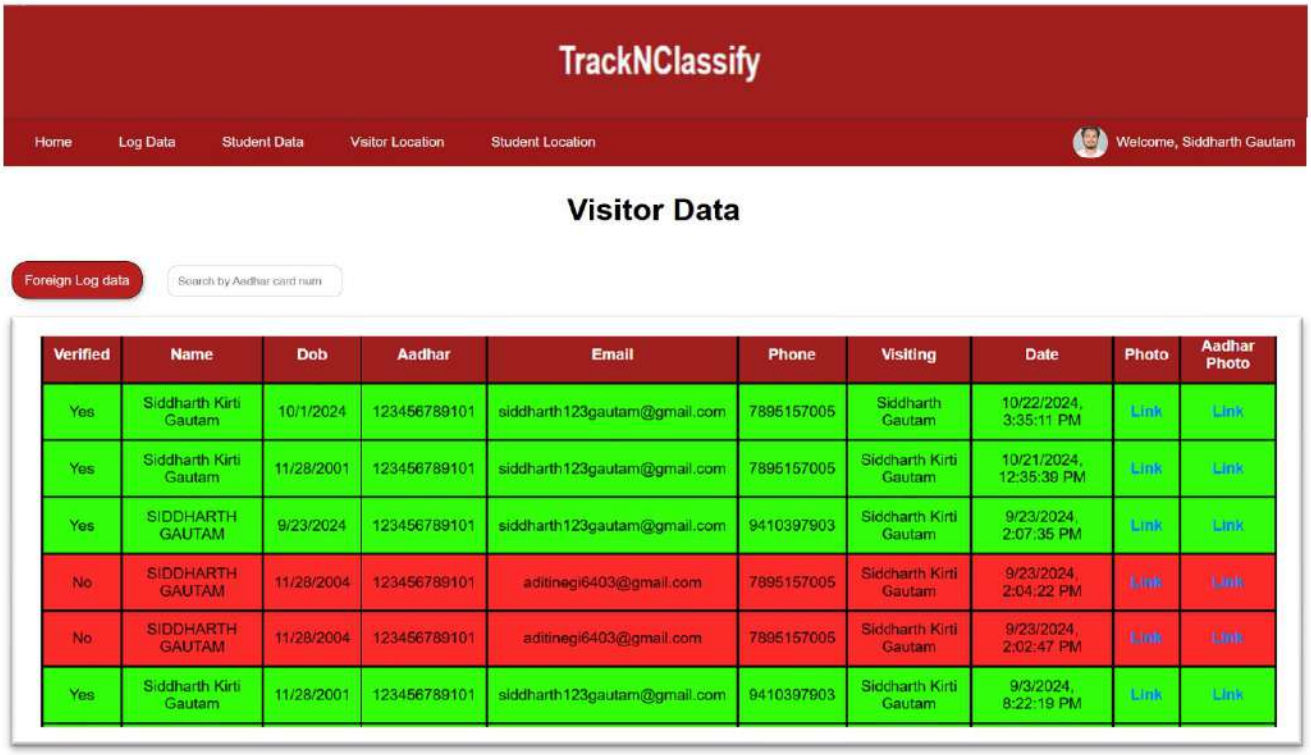


Fig: Visitor Data After being Authenticated (Yes/No)

Fig: Assigning of RFID Number Visitor Pass to the Visitor

Fig: Easy Visualization of Real Time Monitoring of Location (Blue/Yellow/White)

11. References

1. Ekarin Suethanuwong, Supachoke Sukkasame. "**An Access Control System using RFID and Face Verification with QR Code-based Enrollment**." published in the International Journal of Applied Information Technology. This journal is part of the ThaiJo (Thai Journals Online) platform, Thailand, 2023.

2. Vandana and N. Kaur. **"A Study of Biometric Identification and Verification System."** Proceedings of 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), India, pp. 60-64, 2021.

3. K. Selvaraj, S. Alagarsamy, and M. Dhilipkumar. "**Raspberry Pi based Automatic Door Control System**." Proceedings of 2021 3rd International Conference on Signal Processing and Communication (ICPSC), India, 2021.

4. Z. Leyu, Z. Xinyou, F. Yunjia, L. Shuyao, B. Jun, and H. Xijia. "**Design and Implementation of RFID Access Control System Based on Multiple Biometric Features."** Proceedings of the 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Chengdu, China, 2021.

5. "The Use of QR Codes in Security Systems," International Journal of Computer Science, 2021.