Access Tracker for Tech Parks: Aliro

A Group Project Submitted for Undergraduate Project-I Lab (BCA581)

2024 -2025

By

GAURAV JAIN (2241129)

HIMANSHI AGARWAL (2241132)

SUMIT ROBERTS EMMANUEL (2241160)

Bachelor of Computer Science

Under the supervision of

GUIDE NAME

DR. SAGAYA AURELIA

1. Problem Definition

1.1 Overview

The Access Control App for Tech Parks enhances security and streamlines access management using Kotlin and machine learning with facial recognition technology. Employees gain secure entry through facial recognition matching with an existing database. Visitors register via the app, specify their purpose, and are approved by the employee they intend to visit. The app supports employee pre-registration and includes two-step verification with time-sensitive entry codes for added security. Movement history tracking provides a comprehensive overview of access activities. Additionally, the app manages vehicle entry by scanning license plates, allocating parking spaces, and guiding visitors to their designated spots, reducing congestion and improving the overall user experience.

1.2 Problem Statement

Tech parks face significant challenges in ensuring secure and efficient access control due to traditional systems relying on ID cards, manual check-ins, and security personnel. These outdated methods lead to security risks from unauthorized access, inefficiencies, long waiting times, and administrative burdens. There is a lack of integrated systems for managing employee and visitor access, resulting in disjointed operations and difficulty coordinating vehicle entry and parking. Additionally, limited visibility and accountability hinder effective tracking and monitoring of access activities. To address these issues, an advanced, integrated access control system utilizing modern technologies like facial recognition and mobile applications is essential to enhance security, streamline processes, and provide comprehensive oversight of access activities within tech parks.

1.3 Key Objectives

- **Enhance Security**: Implement robust facial recognition technology to ensure secure access control for employees and visitors within tech parks.
- **Streamline Access Management**: Facilitate seamless employee entry through facial recognition matching with a pre-existing database.
- **Visitor Registration and Approval**: Enable visitors to register their visit details via the app, linking their visit to an employee and requiring approval for access.
- **Employee-Driven Access Control**: Allow employees to pre-register visitors for direct access on specified dates.
- **Two-Step Verification**: Introduce an additional layer of security with time-sensitive entry codes that must be entered within a specific time window after the visitor's facial scan.
- **Reduce Administrative Burden**: Minimize the manual work of managing visitor logs and employee access by automating these processes through the app.
- **Vehicle and Parking Management**: Implement license plate recognition for visitors' vehicles. Allocate parking spaces in the visitors' parking lot and provide this information via the app.

1.4 System Components

- **Employee Access Control**: The employee access control system uses a facial recognition system linked to a database of employee facial data for secure and efficient entry.
- **Visitor Management**: Visitor management includes app-based registration and facial recognition entry, supported by employee notifications for visit approval and pre-registration options, alongside two-step verification with time-sensitive entry codes for enhanced security
- **Movement History Tracking**: Movement history tracking logs and monitors access activities for both employees and visitors within the tech park, providing a comprehensive record for security and operational purposes.
- **Vehicle Entry Management**: Vehicle entry management involves scanning visitors' license plates upon arrival, allocating parking spaces in designated areas, and providing in-app guidance to streamline the parking process within the tech park.

1.5 Expected Benefits

- **Enhanced Security**: Facial recognition technology reduces unauthorized access by ensuring only registered individuals can enter, minimizing security breaches.
- **Improved Efficiency**: Automated check-ins and quick facial recognition scans decrease waiting times, streamlining the entry process for employees and visitors.
- **Better User Experience**: A user-friendly mobile app simplifies registration and access, offering a seamless experience for both employees and visitors.
- **Effective Monitoring**: Comprehensive tracking of movement history and access activities allows for better oversight and quick response to security incidents.
- **Resource Optimization**: Automating access control reduces the need for manual interventions, allowing security personnel to focus on more critical tasks and optimizing parking space allocation.

2. *Requirement Specifications*

Sources of Requirements	Requirements Specification
Stakeholder Input: • **Tech Park Management**: Insights on security needs, access control policies, and operational challenges. • **Companies within the Tech Park**: Requirements for employee access, visitor management, and integration with existing security systems. • **Employees and Visitors**: Feedback on current access processes, user experience pain points, and desired features.	**Facial Recognition App:** • Installed app at entry points for accurate facial scanning. • Servers with sufficient processing power for real-time facial recognition.

Regulatory and Compliance Standards: • **Local Security Regulations**: Adherence to laws and guidelines governing access control and data privacy. • **Industry Standards**: Best practices for implementing secure and efficient access control systems.	**Network Infrastructure:** • Reliable and high-speed internet connectivity for data transmission between devices and servers. • Secure and redundant network setup to ensure continuous operation.
Technical Feasibility: • **Technology Providers**: Capabilities of facial recognition systems, mobile application platforms, and machine learning algorithms. • **IT Department**: Integration with existing infrastructure, network requirements, and system compatibility.	**Mobile Devices:** • Smartphones or tablets for users to install and use the app. • Compatibility with the latest versions of Android.
Competitive Analysis: • **Market Research:** Analysis of similar access control solutions, identifying strengths and weaknesses. • **User Reviews:** Insights from user experiences with competitor products.	**Physical Security Infrastructure:** • Integration with existing gates, turnstiles, and access points within the tech park. • Implementation of vehicle license plate recognition systems for parking management.

3. *Functional Requirements*

Req No.	**Requirement**	**Specific Example**
FR01	**User Interaction:** How users will interact with the system, what actions they can perform, and what outputs they can expect.	The system must allow employees to gain entry through facial recognition matching with an existing database, ensuring secure and efficient access. Visitors must register via the app, specifying their purpose and the employee they intend to visit, with notifications sent to the associated employee for approval.
FR02	**Data Processing:** How data will be collected, stored, processed, and presented within the system.	The system should store facial recognition data securely and process it in real time for immediate access decisions.

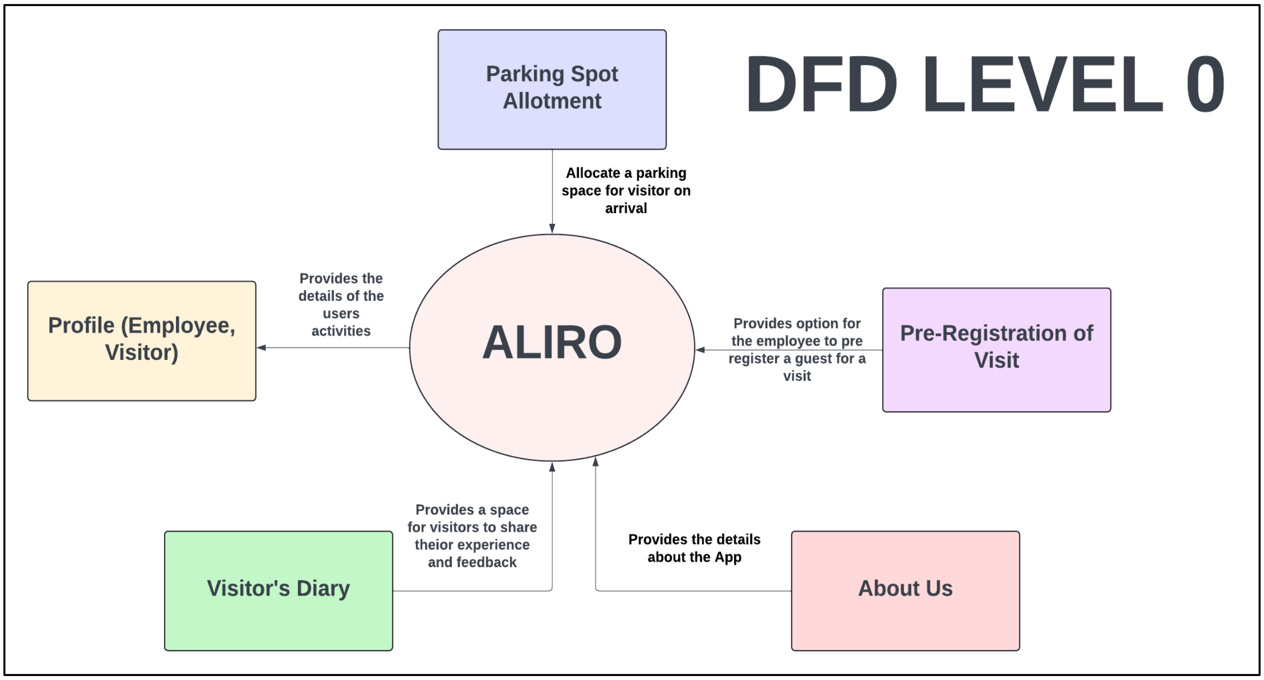
		Visitor information, including purpose and visit history, should be stored and accessible to authorized personnel.
FR03	**System Behavior:** Describing how the system should respond to various inputs and perform different tasks.	The system should send notifications to employees when a visitor arrives and requests access. It should provide real-time updates on the status of access requests and entry approvals.
FR04	**System Components:** Identifying the various modules, components, or features that make up the system.	The system must include a facial recognition module for employee and visitor identification. It should feature a visitor registration module allowing visitors to specify their purpose and the employee they intend to visit. The system should have a notification module to alert employees of visitor arrivals and access requests.
FR05	**Performance:** Defining performance metrics such as response times, processing speed, and capacity to handle concurrent users.	The system should process facial recognition data within seconds to minimize entry wait times. It must handle multiple simultaneous access requests efficiently, ensuring no delays in user experience.
FR06	**Integration:** Addressing how the system will integrate with other existing systems or databases.	The system should integrate with existing employee databases to verify facial recognition matches. It should be able to communicate with security systems to log entry and exit times accurately.
FR09	**Security:** Specifying the measures that ensure data security, access control, and protection against unauthorized access.	The system must implement robust encryption protocols to protect sensitive facial recognition data. It should include two-step verification for visitors, using time-sensitive entry codes to enhance security. Access to data should be restricted to authorized personnel only, with strict authentication measures in place.

4. *System Requirements*

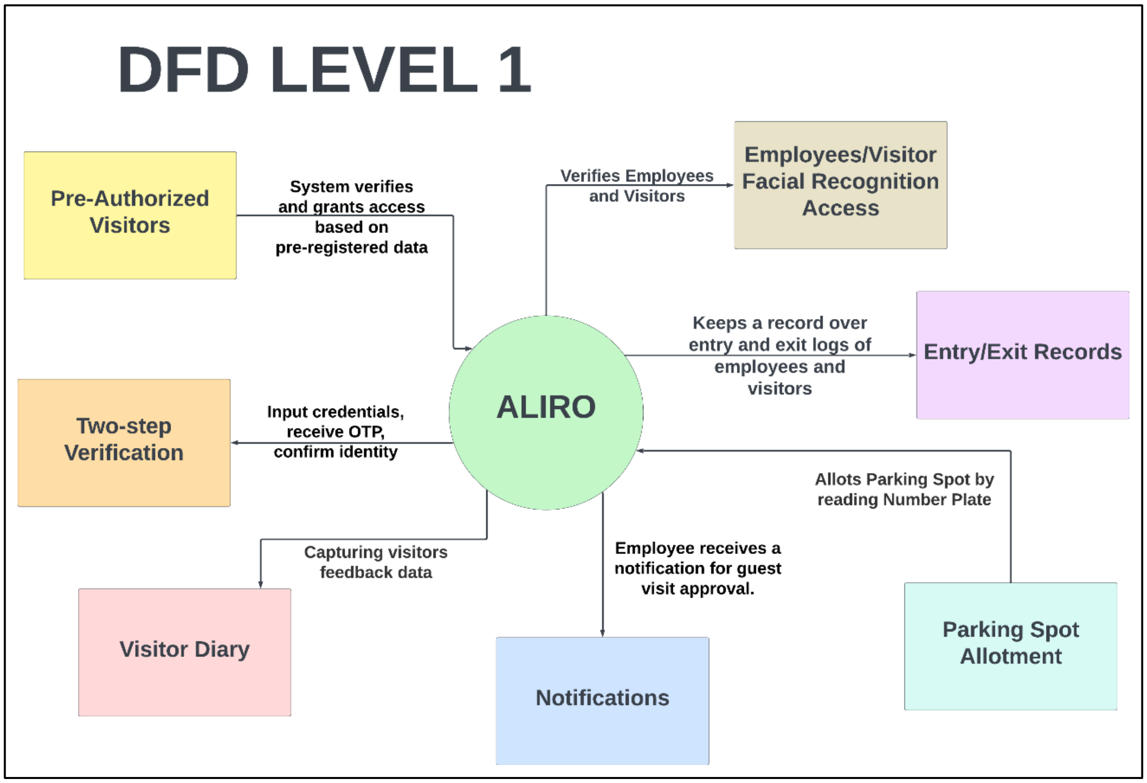
Hardware Requirements	Software Requirements	Other Requirements
• **Processor**: Multi-core processors, preferably Intel Xeon or AMD EPYC, with at least 8 cores. • **Memory (RAM)**: Minimum 32 GB RAM. • **Power Supply**: Redundant power supplies to ensure continuous operation even in case of a power failure. • **Internet Connectivity**: High-speed internet connection with at least 100 Mbps bandwidth. • **Mobile Devices**: Android	• **Operating System**: Android for mobile devices and Windows server and administrative systems. • **Facial Recognition Library**: TensorFlow • **Database**: SQLite • **API Integration**: Amazon Image Rekognition • **Language**: Kotlin	• Regulatory Compliance • User Training and Support

5. *ConceptualModels*

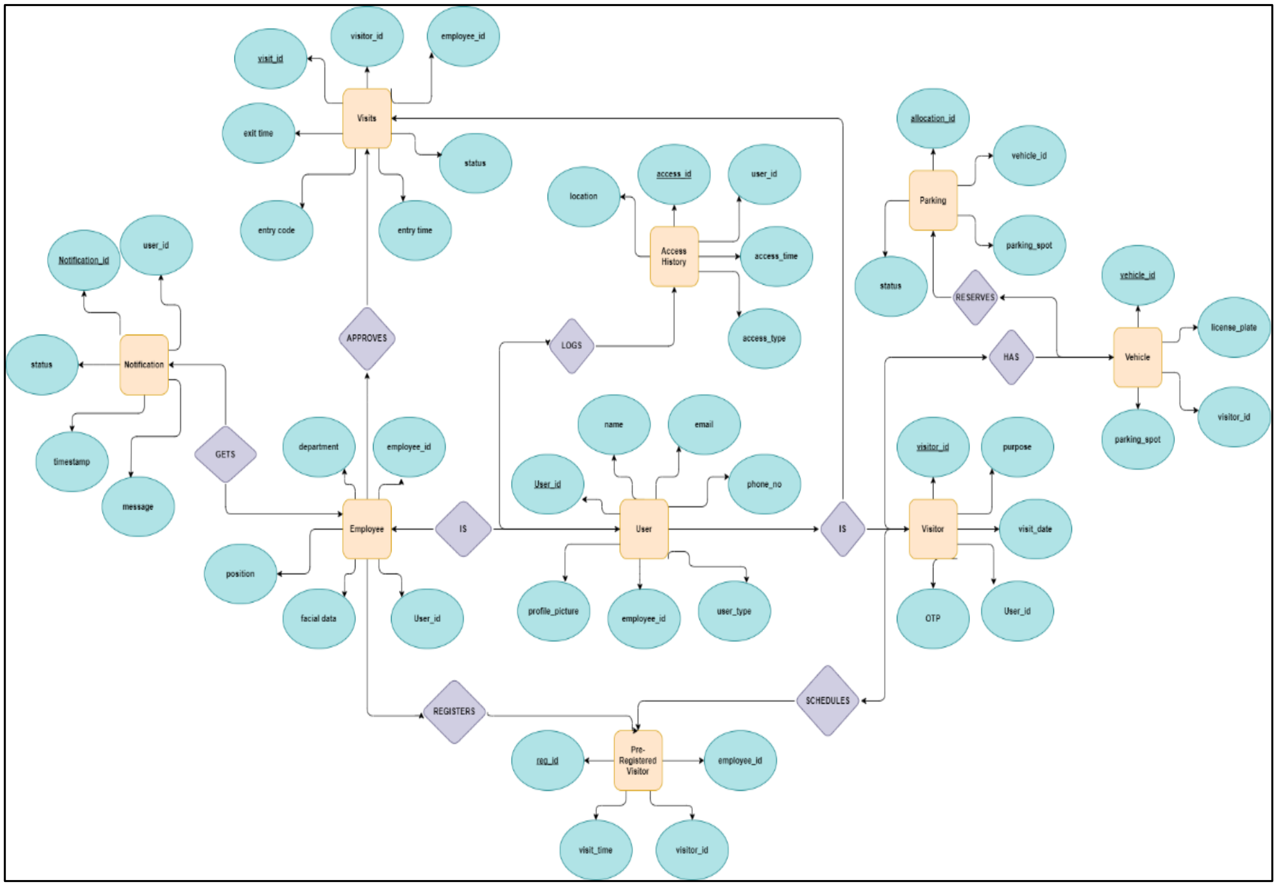
5.1 Data Flow Diagram



DFD LEVEL 0
Parking Spot Allotment
Allocate a parking space for visitor on arrival
Provides the details of the users activities
Profile (Employee, Visitor)
ALIRO
Provides option for the employee to pre register a guest for a visit
Pre-Registration of Visit
Provides a space for visitors to share theior experience and feedback
Visitor's Diary
Provides the details about the App
About Us


DFD LEVEL 1
Pre-Authorized Visitors
System verifies and grants access based on pre-registered data
Verifies Employees and Visitors
Employees/Visitor Facial Recognition Access
ALIRO
Keeps a record over entry and exit logs of employees and visitors
Entry/Exit Records
Two-step Verification
Input credentials, receive OTP, confirm identity
Allots Parking Spot by reading Number Plate
Capturing visitors feedback data
Employee receives a notification for guest visit approval.
Visitor Diary
Notifications
Parking Spot Allotment

5.2 ER DIAGRAM


visit_id
visitor_id
employee_id
Visits
exit time
status
entry code
entry time
location
access_id
user_id
Access History
access_time
access_type
allocation_id
vehicle_id
Parking
parking_spot
status
RESERVES
vehicle_id
license_plate
Vehicle
HAS
visitor_id
parking_spot
Notification_id
user_id
status
Notification
timestamp
message
GETS
APPROVES
LOGS
department
employee_id
Employee
IS
position
facial data
User_id
name
email
User_id
phone_no
User
profile_picture
employee_id
user_type
IS
visitor_id
purpose
Visitor
visit_date
OTP
User_id
REGISTERS
SCHEDULES
reg_id
Pre-Registered Visitor
employee_id
visit_time
visitor_id