

Face recognition Lock System design

PERIOD 4



April 26, 2024

GROUP H

Contents

[CHAPTER I. INTRODUCTION 2](#_Toc165026154)

[CHAPTER II. OBJECTIVES 3](#_Toc165026155)

[CHAPTER III. BOUNDARIES. 4](#_Toc165026156)

[CHAPTER IV. SOFTWARE DESIGN. 5](#_Toc165026157)

[CHAPTER V. SYSTEM ARCHITECTURE. 6](#_Toc165026158)

[CHAPTER VI. FLOW CHART 13](#_Toc165026159)

[CHAPTER VII. UI/UX DESIGN. 13](#_Toc165026160)

[CHAPTER VIII. COSTS. 13](#_Toc165026161)

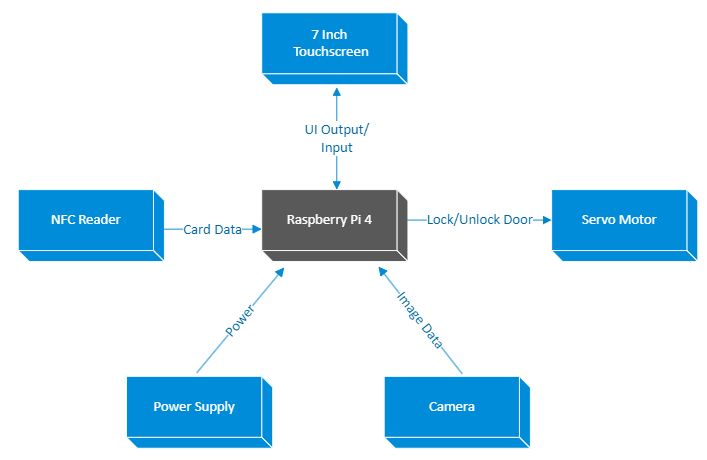
[APPENDIX. 15](#_Toc165026162)

# CHAPTER I. INTRODUCTION

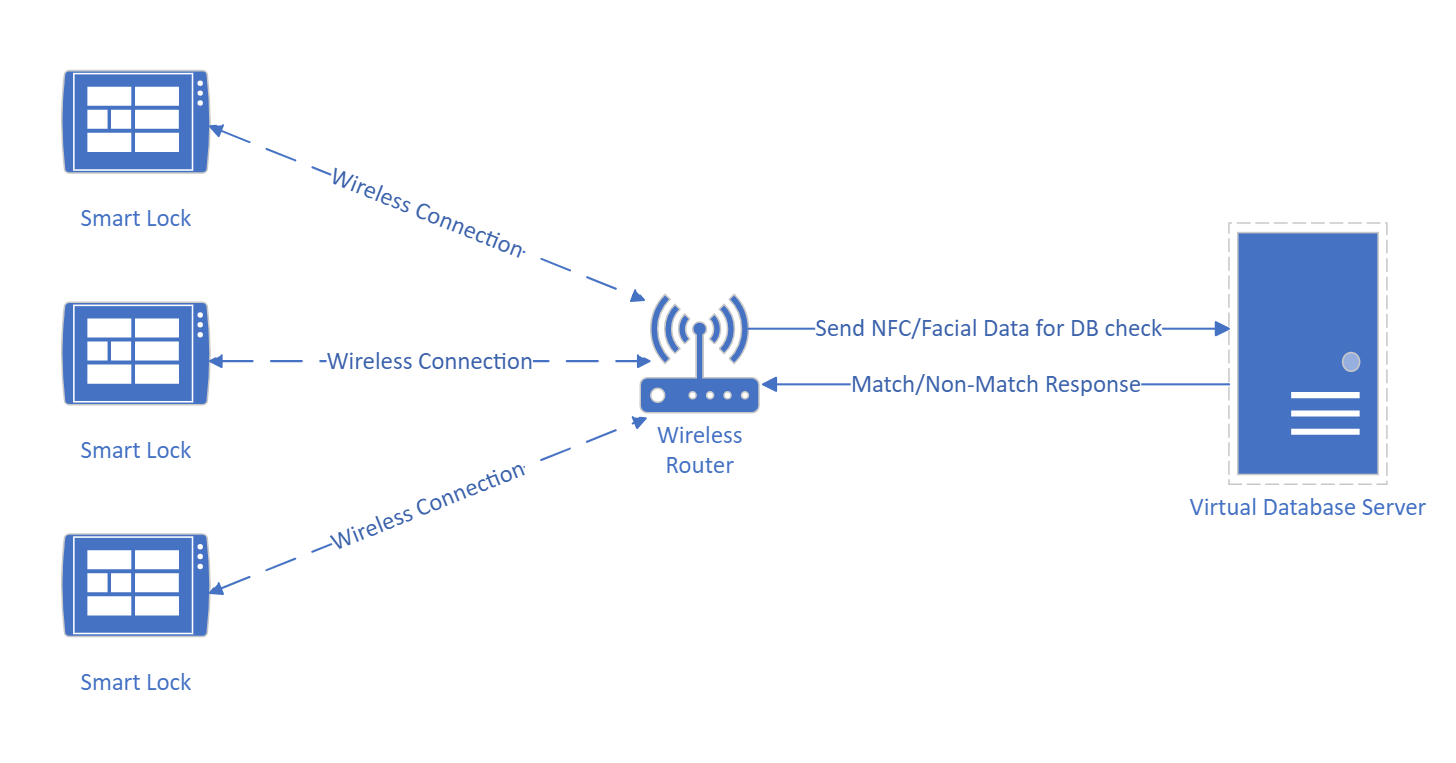
The Smart Lock System project is a forward-looking initiative aimed at revolutionizing access control within corporate or academic settings. Our main objective is to seamlessly integrate facial recognition technology with NFC scanning capabilities, ensuring that only authorized individuals gain entry. With this advanced system installed at every entry point throughout the organization, we seek to address concerns related to unauthorized access and security breaches.

Furthermore, our innovative strategy goes beyond conventional security measures. By connecting the smart lock technology to Wi-Fi, we establish a dynamic link to a virtual machine (VM) housing the database. This connectivity enables real-time data transmission, bolstering the system's responsiveness and efficiency.

Our dedicated team has invested considerable time and effort into this project, recognizing the pressing need for enhanced security protocols in diverse environments. Through the fusion of biometric authentication and NFC scanning, we aim to simplify the entry process for users while fortifying overall security measures.



***Image 1. Smart lock system***

 ***Image 2. Lock communication with central database***

# CHAPTER II. OBJECTIVES

**Overview**

The objective of this project is to develop a secure, efficient, and user-friendly smart lock system for our university. Utilizing facial recognition technology integrated with NFC scanning capabilities, this system aims to enhance building security while providing convenient access control.

**Specific Objectives**

1. **Security Enhancement**:

* To deploy a system that strengthens the security of university/company facilities by ensuring that only authorized individuals gain access.
* To maintain an accurate log of all entry and exit events for security auditing and real-time monitoring.

1. **Operational Efficiency**:

* To streamline the process of room booking and access control, reducing the administrative workload and wait times for users.
* To enable immediate access upon successful biometric authentication, thus saving time compared to traditional lock-and-key methods.

1. **User Convenience**:

* To offer multiple authentication methods (facial recognition and NFC card) to accommodate user preferences and contingencies.
* To create an intuitive UI/UX that simplifies the interaction with the smart lock for users of varying technical proficiency.

1. **Integration and Compatibility**:

* To ensure the smart lock system's compatibility with existing university infrastructure and potential future technology integrations.
* To design the system in a way that allows for easy updates and scalability to accommodate the university's evolving needs.

1. **Innovation and Technology Advancement**:

* To utilize cutting-edge technologies such as facial recognition and NFC to position our university at the forefront of technological innovation in campus security.
* To demonstrate a model that could serve as a benchmark for similar systems in educational institutions or corporate settings.

1. **Compliance and Privacy**:

* To ensure the system adheres to privacy regulations and ethical standards concerning biometric data.
* To implement strict data management protocols to protect user information.

**Deliverable Focus**

The project will deliver a fully functional prototype that embodies the objectives listed above. The prototype will serve as a testament to the feasibility and benefits of integrating advanced biometric technology into daily campus operations.

# CHAPTER III. BOUNDARIES.

The project aims to develop a face recognition-based locking system for securing access to designated spaces, such as rooms or buildings. Leveraging facial recognition technology, the system will authenticate authorized individuals and grant access while deterring unauthorized entry. Primarily, the project will concentrate on software development and the integration of compatible hardware components, focusing on demonstrative purposes.

**3.1. Timeline:**   
Spanning nine weeks, from April 22, 2024, to June 21, 2024.

**Week 1-2 (April 22 - May 3, 2024):**

During the initial two weeks, the focus will be on conducting comprehensive research related to facial recognition technology, NFC scanning, and smart lock systems. Additionally, team members will utilize this time to enhance their proficiency in Python programming language and explore relevant libraries such as OpenCV, dlib, and PyMySQL. Documentation preparation, including project scope, objectives, and initial system architecture, will also commence during this period.

**Week 3 (May 4 - May 10, 2024):**

In the third week, the emphasis will be on finalizing the selection of hardware components required for the face recognition lock system. Detailed specifications and procurement plans will be developed, ensuring compatibility and availability of the necessary equipment. Meanwhile, the software design phase will commence, outlining the structure and functionality of the proposed system.

**Week 4-5 (May 11 - May 24, 2024):**

With the hardware components procured, the development phase will intensify during weeks four and five. Team members will work on implementing the facial recognition algorithm using OpenCV and dlib libraries. Simultaneously, database schema design and setup using MySQL will be undertaken, laying the foundation for user data management. Progress will be documented, and any challenges encountered will be addressed promptly.

**Week 6 (May 25 - May 31, 2024):**

In the sixth week, attention will be directed towards integrating the developed software modules with the acquired hardware components. Initial testing and debugging will be conducted to ensure compatibility and functionality. User interface (UI) design concepts will also be explored, aiming for an intuitive and user-friendly interaction experience.

**Week 7 (June 1 - June 7, 2024):**

As the project enters its penultimate phase, the focus will shift towards refining the system's functionality and user interface based on feedback from initial testing. Attention will be given to optimizing performance, enhancing security features, and addressing any identified vulnerabilities. Additionally, preparations for the final product demonstration and documentation completion will be initiated.

**Week 8 (June 8 - June 14, 2024):**

The eighth week marks the finalization of the face recognition lock system prototype. Comprehensive testing and validation will be conducted to ensure the system meets the predefined requirements and specifications. Final adjustments and enhancements will be made based on user feedback and usability testing results. The project deliverables, including software, documentation, and presentation materials, will be prepared for submission.

**Week 9 (June 15 - June 21, 2024):**

During the last week of the project, the focus will be on receiving feedback from stakeholders, including project supervisors and potential end-users. Any necessary refinements or adjustments to the system will be implemented based on the feedback received. Final documentation updates and project wrap-up activities, including post-mortem analysis and future recommendations, will be completed to conclude the project successfully.

**3.2. Deliverables:**

* A functional prototype of the face recognition lock system.
* Software encompassing facial recognition algorithm implementation and user interface.
* Comprehensive documentation detailing system architecture, installation procedures, and user manual.
* Presentation materials to showcase the system's functionality and features.

**3.3. Key Features:**

* Facial Recognition: Accurately identifies authorized individuals based on facial characteristics.
* User Database Management: Allows registration, updating, and removal of authorized users from the system.
* Access Control: Grants or denies access based on recognition results and user permissions.
* Logging and Reporting: Records access attempts and generates reports for review and analysis.

**3.4. Constraints:**

* Sole focuses on software development, utilizing existing hardware components for testing and demonstration.
* Integration with third-party hardware devices limited to compatibility and feasibility within the project timeframe.
* The system will not address advanced security measures such as encryption or remote network connectivity.
* Accuracy and performance of the facial recognition algorithm may be constrained by available computational resources and training data.
* The project will not involve purchasing a completed smart lock from the market, as the software may be locked due to security purposes. Instead, components will be ordered online to construct a smart lock system. The system will function such that the latch opens only when facial recognition and information on the student card (e.g., student number, name) match those in the database. The lock will default to a locked state at all other times.

# CHAPTER IV. SOFTWARE DESIGN.

This chapter offers an overview of the diverse technologies integral to constructing our software solution. From the core programming language to database administration, and from image manipulation to interfacing with hardware, we will examine the tools and libraries essential to our project. Whether it involves managing employee data, deploying facial recognition, or connecting with hardware elements like NFC scanners and door locks, each technology is indispensable in achieving the functionality of our system.

### **Summary of Key Components and Libraries:**

#### **Programming Language**

**Python**:Python is the primary programming language used for developing the software. It is installed on the Raspberry Pi to handle various functionalities, including image processing, database interactions, and hardware interfacing. Additionally, Python is used to design and code the admin application, which manages employees, performs facial recognition, and handles NFC authentication.

#### **Database Interaction**

* **Microsoft SQL Server**: Used to store employee data, including their IDs, pictures, and other relevant information.
* **SQLAlchemy**: A Python SQL toolkit and Object-Relational Mapping (ORM) library. It is used to interact with the Microsoft SQL Server database, providing a high-level abstraction upon the database engine and simplifying database operations.
* **PyMSSQL**: A Python library that provides a database interface for Microsoft SQL Server. It is used to directly connect and execute queries against the SQL Server database.

#### **Graphical User Interface (GUI)**

* **PyQt**: A set of Python bindings for Qt libraries, used to create graphical user interfaces (GUIs). It is used in this project to create the desktop application for managing employees, performing facial recognition, and handling NFC authentication.

#### **Facial Recognition**

* **OpenCV**: Essential for face recognition. It provides various functionalities for image processing and computer vision tasks. It is used to capture images from the camera and perform facial recognition tasks.
* **Dlib**: A powerful library for machine learning, which includes facial recognition capabilities. It provides pre-trained models for face detection and facial landmark detection, which are used in conjunction with OpenCV for face recognition.
* **Face Recognition**: A library built on top of Dlib, providing easy-to-use functions for detecting and recognizing faces in images. It is used to encode and compare facial data.
* **Pillow (PIL)**: Useful for image processing tasks. It is used to manipulate images, such as resizing, cropping, or converting between different image formats.
* **Picamera2**: Used to interface with the Raspberry Pi camera module, capturing images for facial recognition.

#### **NFC Interaction**

* **NFCpy**: A Python library that allows interaction with NFC devices, such as NFC tags and readers. It is used to read data from NFC tags for authentication purposes.

#### **Password Security**

* **Bcrypt**: A library used for password hashing. It is used in the admin application to securely store and verify administrator passwords.

# CHAPTER V. SYSTEM ARCHITECTURE.

This chapter provides an extensive list of hardware components crucial for the door unlocking system. Each component is individually outlined, complemented by accompanying images for visual clarity. The detailed breakdown aims to enhance understanding of the necessary components, making acquisition and setup more straightforward.

5.1 Hardware List

* Raspberry Pi 4 – 4GB
* Raspberry Pi Camera 2
* Raspberry Pi 7 inch 800x480 DSI Touchscreen Display
* Raspberry Pi Display Cable - Standard-Mini – 200mm
* PN532 NFC/RFID controller breakout board - v1.6
* 13.56MHz RFID/NFC card – 1KB
* Grove – Servo
* Power Supply / Connectivity to socket

5.2 Subsystem architecture

**5.2.1. Raspberry Pi 4 – 4GB**

The core decision-making system of the door unlocking mechanism is housed within the Raspberry Pi 4 - 4GB microcomputer. This powerful processor manages authentication requests from the RFID/NFC sensor or analyzes visual input from the camera to determine whether access should be granted or denied.

A circuit board with many wires

Description automatically generated

***Image 3. Raspberry Pi 4 – 4GB***

**5.2.2. The Raspberry Pi Camera 2**

The Raspberry Pi Camera 2 acts as the key authentication tool for door access. It records images or video clips of individuals approaching the door, serving as the main method to confirm their legitimacy. Only those successfully identified through the camera's visuals are granted entry, guaranteeing access solely to authorized individuals. Additionally, the recorded footage allows for remote monitoring of access attempts, offering real-time surveillance of the premises' security status.

A small green circuit board with a white ribbon

Description automatically generated

***Image 4. The Raspberry Pi Camera 2***

**5.2.3. Raspberry Pi 7 inch 800x480 DSI Touchscreen Display**

Raspberry Pi 7 inch 800x480 DSI Touchscreen Display: This touchscreen display provides a user-friendly interface for configuring the door unlocking system.

A tablet next to a box

Description automatically generated

***Image 5. Raspberry Pi 7 inch 800x480 DSI Touchscreen Display***

**5.2.4.** **The Raspberry Pi Display Cable - Standard-Mini - 200mm**

The Raspberry Pi Display Cable - Standard-Mini - 200mm is an component that facilitates the connection between the Raspberry Pi microcomputer and the touchscreen display.

A close-up of a computer cable

Description automatically generated ***Image 6. The Raspberry Pi Display Cable - Standard-Mini - 200mm***

**5.2.5.** **PN532 NFC/RFID Controller Breakout Board & 13.56MHz RFID/NFC card**

PN532 NFC/RFID Controller Breakout Board: Integrated with a 13.56MHz RFID/NFC card reader, this sensor detects authorized RFID tags or NFC-enabled devices. When a valid tag is presented, the system grants access by activating the door unlocking mechanism.

A blue circuit board with small pins and a white card

Description automatically generated ***Image 7. PN532 NFC/RFID Controller Breakout Board & 13.56MHz RFID/NFC card***

**5.2.6.** **Grove – Servo**

The Grove - Servo module is essential for automating door functions, enabling precise opening and closing movements. When integrated into door control systems, this servo motor provides the necessary mechanical force to operate the door mechanism smoothly and accurately.

A small electronic device with wires and screws

Description automatically generated

***Image 8. Grove – Servo***

**5.2.7.** **The Power Supply / Connectivity to socket**

The Power Supply / Connectivity to socket part is like the heart of the system, making sure everything stays running by giving power to all the connected devices. Whether it's plugged into a socket or using a battery, this part keeps the whole system working.

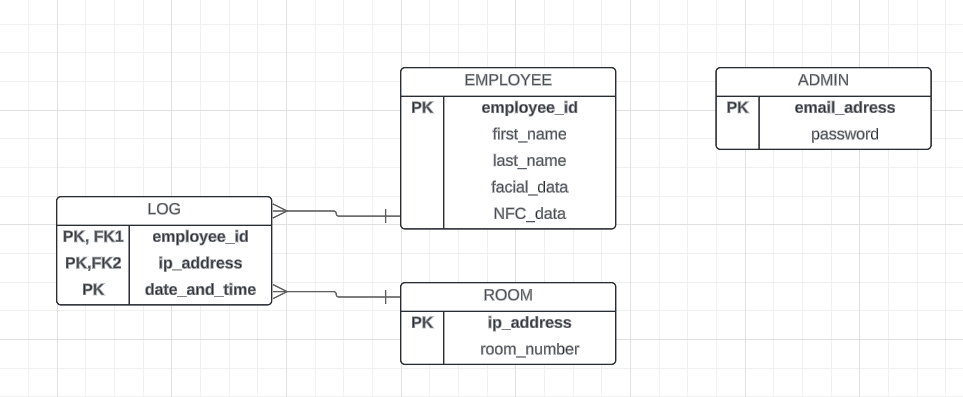
A white charger with a wire

Description automatically generated ***Image 9. The Power Supply / Connectivity to socket***

# CHAPTER VI. SYSTEM DESIGN DIAGRAMS

**6.1. Entity Relationship Diagram (ERD)**

The ERD provides a visual representation of the database structure for the Face Recognition Lock System. It illustrates the relationships between different entities within the system and highlights how data is interconnected. The key entities in this system are EMPLOYEE, ADMIN, ROOM, and LOG.



**ERD Explanation:**

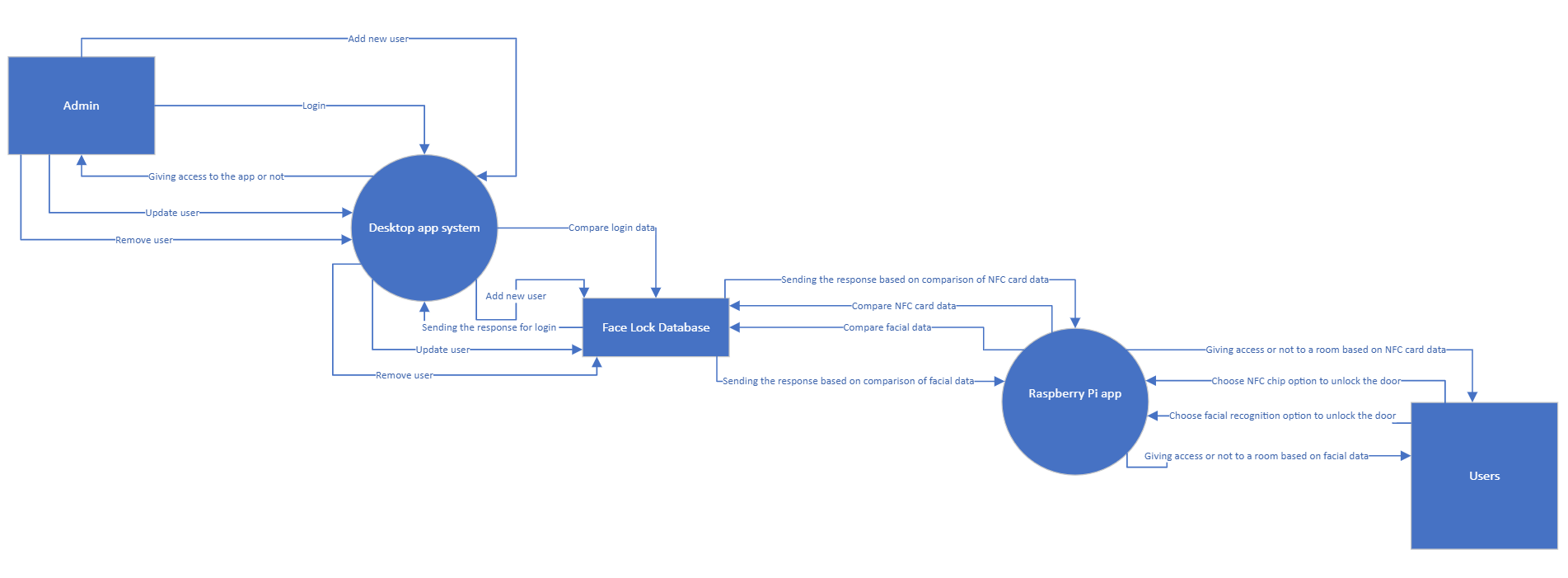
* **EMPLOYEE**: This entity stores information about employees, including their unique ID, first name, last name, facial data (stored as a binary large object - BLOB), and NFC data (string type for storing NFC card details).
* **ADMIN**: This entity stores information about administrators, including their email address and password, used for managing the system.
* **ROOM**: This entity stores information about rooms, including the IP address and room number.
* **LOG**: This entity records all access attempts, including the employee ID, IP address of the room accessed, and the date and time of the attempt.

The relationships are as follows:

* **EMPLOYEE** to **LOG**: One-to-Many (One employee can have multiple log entries)
* **ROOM** to **LOG**: One-to-Many (One room can have multiple log entries)
* **ADMIN**: Independent entity used for system management.

**6.2. Data Flow Diagram (DFD) Level 1**

The DFD Level 1 provides an overview of how data flows through the system, from user interaction to database storage and vice versa. It highlights the key processes and data stores involved in the system.



**DFD Explanation:**

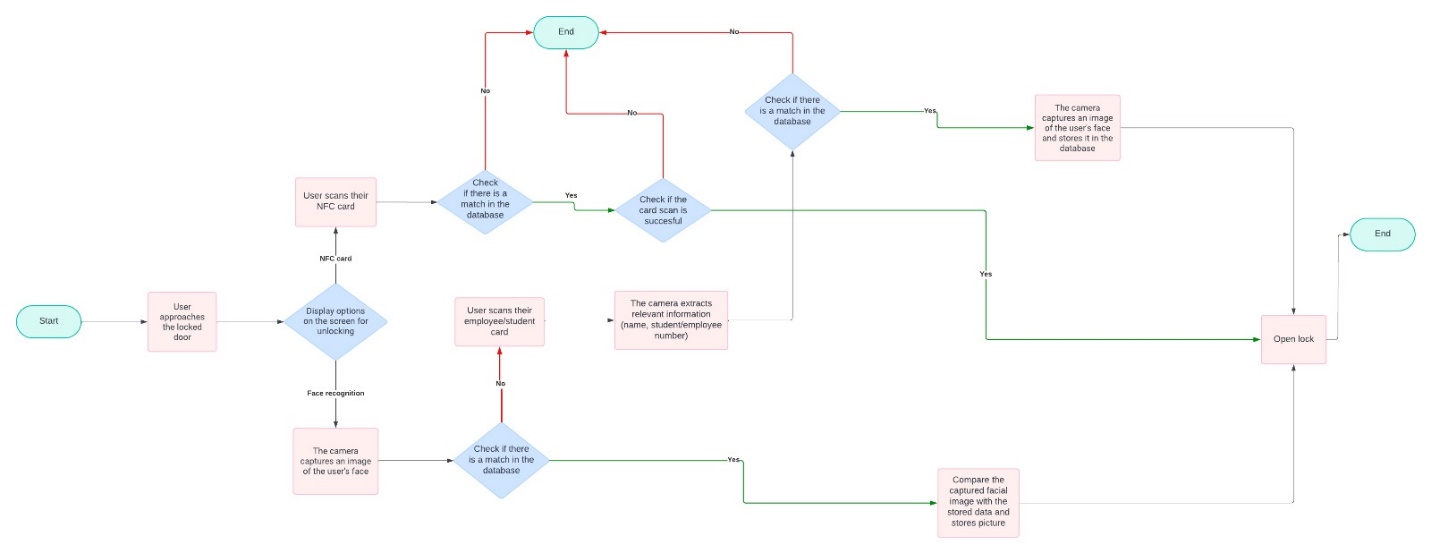
* **Admin**: The admin can log in, add new users (employees), edit or remove users, and manage the system through a desktop application.
* **Desktop App System**: This system handles all user management functionalities, compares login data, and interacts with the database to update or retrieve information.
* **Face Lock Database**: The central database that stores all data related to employees, admins, rooms, and access logs.
* **Raspberry Pi App**: This application runs on the Raspberry Pi, interfacing with the facial recognition and NFC scanning hardware. It authenticates users and sends access requests to the database.
* **Users**: Employees who use the system to gain access to rooms. Their authentication data is compared against the stored records in the database.

The flow involves:

1. **Admin** logging in and managing users through the **Desktop App System**.
2. **Desktop App System** interacting with the **Face Lock Database** to add, update, or remove user records.
3. **Users** attempting to access rooms using the **Raspberry Pi App**, which sends authentication data to the **Face Lock Database**.
4. The **Face Lock Database** validating the data and sending a response back to the **Raspberry Pi App** to grant or deny access.
5. **LOG** entries being created for each access attempt, detailing the employee ID, room-specific smart lock’s IP address, and timestamp.

#### **6.3. Flowchart for User Authentication Process**

The flowchart illustrates the detailed process flow for user authentication using the Face Recognition Lock System. It demonstrates the steps involved from the moment a user approaches the locked door to the point where access is granted or denied.

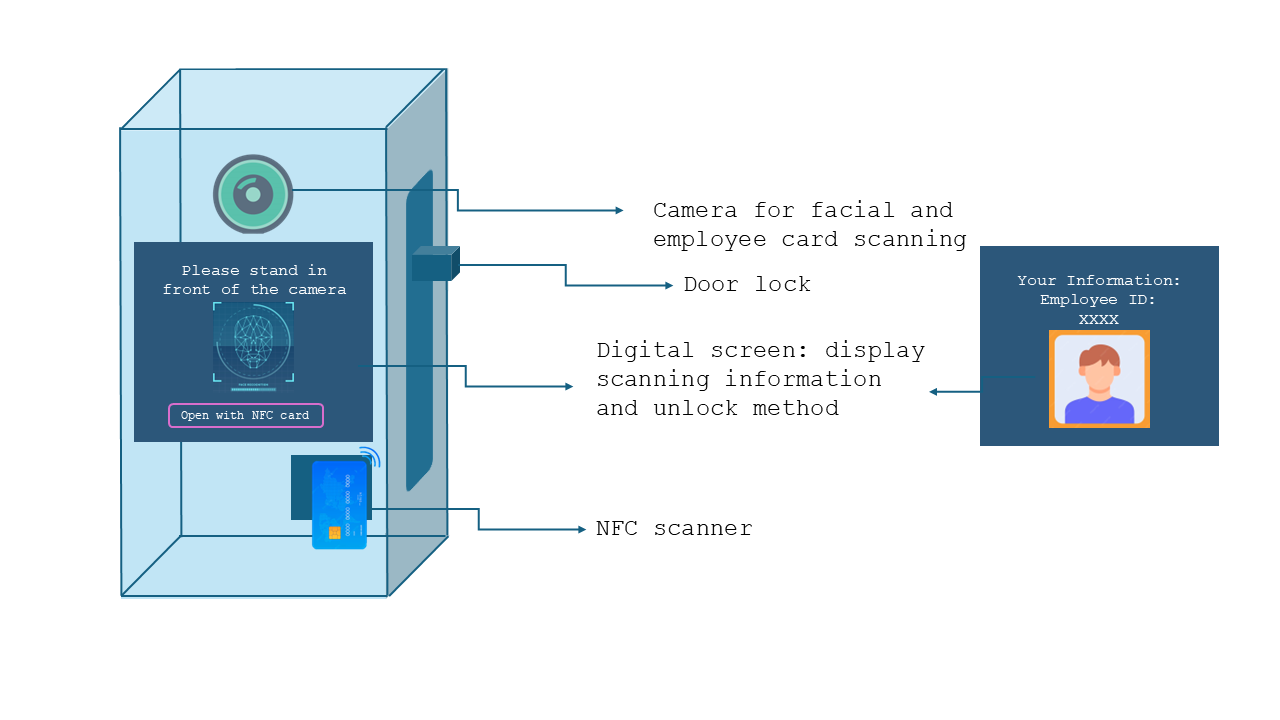


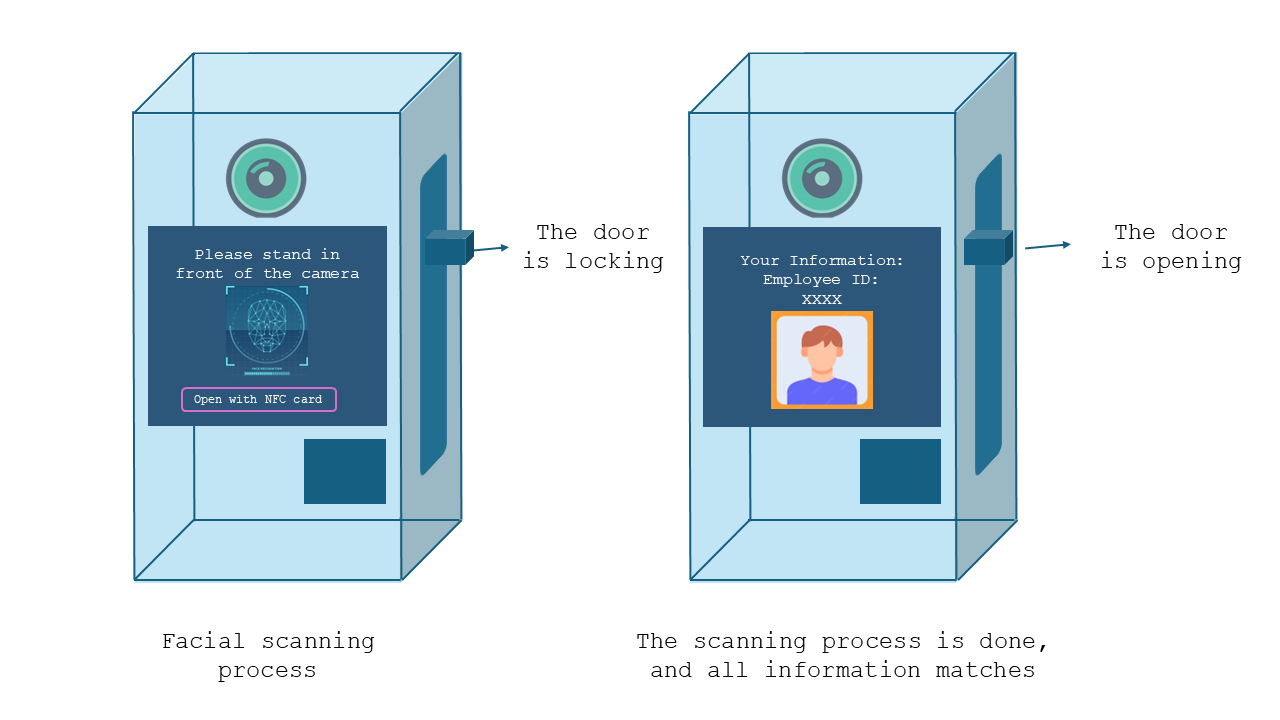
**6.4. Raspberry Pi Pinout Diagram**



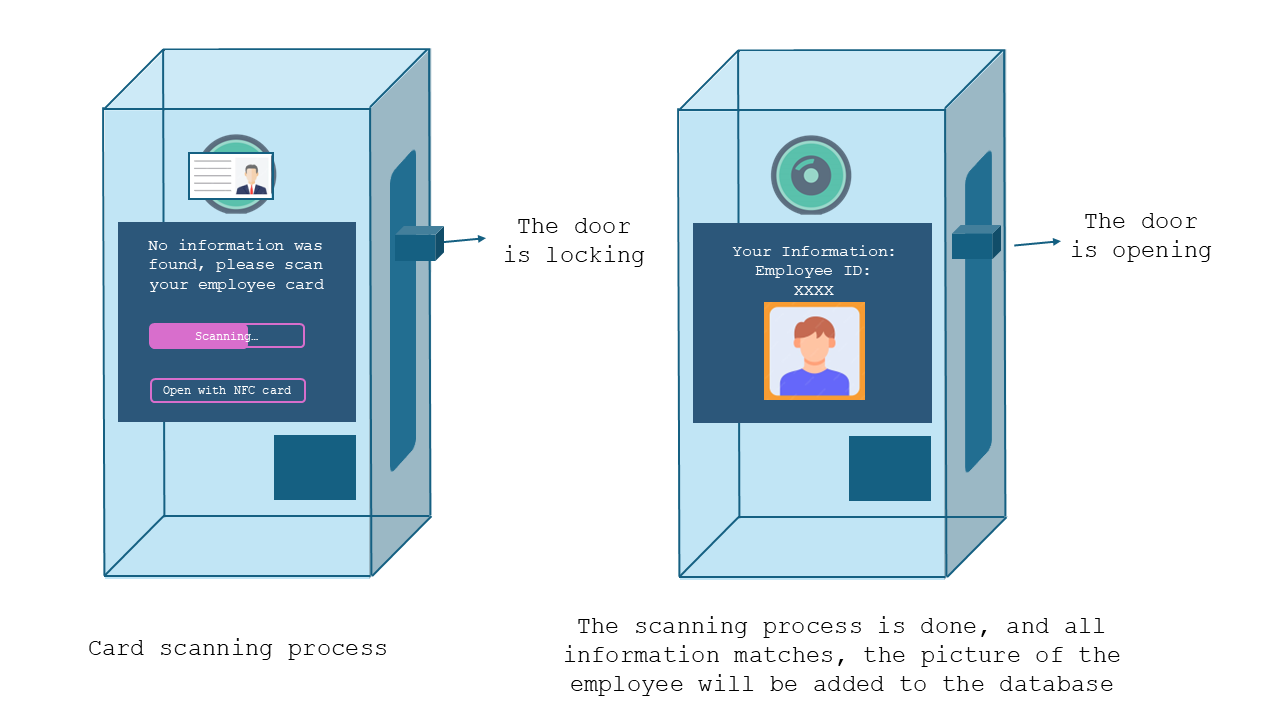
|  |  |  |
| --- | --- | --- |
| **Raspberry Pi Pin** | **Component Pin** | **Component name** |
| D2, D14, DSI port | 5V – D2, GND – D14, DSI display connector | Raspberry pi touchscreen |
| D4, D6, D12 | 5V – D4, GND – D6, Output – D12 | Servo motor |
| DSI port | DSI camera connector | Pi camera v2 |
| USB port | USB | NFC Reader ACR122U |
| USB-C port | USB-C – USB | Power supply |

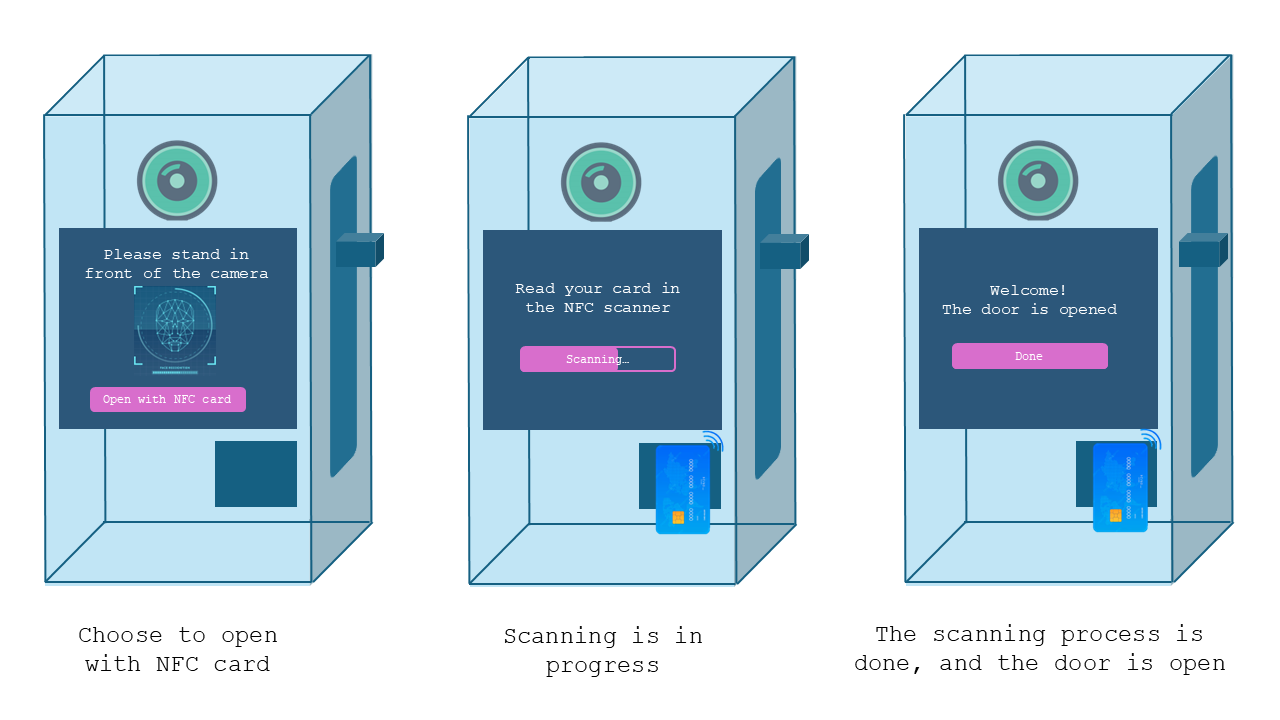
# CHAPTER VII. UI/UX DESIGN.



***Image 10, 11. The exterior design of the smart lock***

***Image 12. The lock operation with facial recognition***



***Image 13. The lock operation with facial recognition and card reading. Card reading will be required if the program cannot recognize the person***

***Image 14. The lock operation with NFC card reading***

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated***Image 15. The desktop application which allows access to the database and train the program to read information on employee cards***

***Image 16. The function training the program to read information on employee cards***

A screenshot of a computer

Description automatically generated

***Image 17. The function to show, import, export, write SQL statements, and view the database structure. The notification will pop up when the unlock process is done***

# CHAPTER VIII. COSTS.

This section outlines the expenses associated with acquiring the necessary hardware components for the door unlocking system.

Costs per component:

|  |  |  |
| --- | --- | --- |
| Name | Price | Link |
| Raspberry Pi 4 – 4GB | € 61.95 | https://www.kiwi-electronics.com/en/raspberry-pi-4-model-b-4gb-4268?search=Raspberry%20Pi |
| Raspberry Pi Camera 2 | € 18.95 | https://www.kiwi-electronics.com/en/raspberry-pi-camera-module-2-8mp-2359?search=pi%20camera%202 |
| Raspberry Pi 7 inch 800x480 DSI Touchscreen Display | € 74,95 | https://www.kiwi-electronics.com/en/raspberry-pi-boards-cases-addons-and-accessories-59/raspberry-pi-7quot-800x480-dsi-touchscreen-display-1948 |
| Raspberry Pi Display Cable - Standard-Mini – 200mm | € 1.25 | https://www.kiwi-electronics.com/en/raspberry-pi-display-cable-standard-mini-200mm-11591?search=display%20kabel |
| PN532 NFC/RFID controller breakout board - v1.6 | € 44,95 | https://www.kiwi-electronics.com/en/pn532-nfc-rfid-controller-breakout-board-v1-6-616?search=nfc |
| 13.56MHz RFID/NFC card – 1KB | € 2,95 | https://www.kiwi-electronics.com/en/13-56mhz-rfid-nfc-kaart-1kb-863?search=nfc |
| Grove – Servo | € 8.25 | https://www.kiwi-electronics.com/en/grove-servo-2070?search=servo%20motor |
| Power Supply / Connectivity to socket | € 14.95 | <https://www.kiwi-electronics.com/en/argon-pwr-gan-usb-c-pd-27w-for-rpi-5-eu-plug-20012?search=power%20supply%20for%20raspberry%20pi%205> |
| Delivery | Free |  |

**Total costs: € 228.2**