Design Document

for

CareConnect

Prepared by Group B7

Table of Contents

1. Considerations 1
1.1 Assumptions 1
1.2 Constraints 1
1.3 System Environment 1
2. Overall Description 2
2.1 Overview 2
2.2 Product Functions 2
2.3 Component Diagrams 2
2.4 Class Diagrams 2
2.5 Data Flow Diagram 2
3. User Interface Design 3
4. User Case Diagram 4
Appendix A: Team members 5

1. Introduction Consideration

1.1 Assumptions

The functioning of the app relies on several key assumptions to ensure its effectiveness. Firstly, it assumes that the person under isolation possesses a properly working smartphone with SMS functionalities. This assumption is vital for the app to monitor phone unlock activity and send timely alerts in case of prolonged inactivity or sudden falls. The app leverages SMS functionalities as part of its communication strategy, allowing for immediate notifications to be sent to emergency contacts and facilitating a rapid response to potential emergencies. Therefore, the assumption of a functional smartphone with SMS capabilities is fundamental to the app's overall functionality.

1.2 User Classes and Characteristics

A critical constraint embedded in the app's design is the incorporation of proper login and user data security measures. This constraint is paramount to safeguarding the privacy and confidentiality of the monitored individual's data. The app must implement robust authentication mechanisms to ensure that only authorized users can access sensitive information related to phone unlock activity. Additionally, user data, including personal information and monitoring logs, must be securely stored and transmitted. Adhering to industry best practices and data protection regulations is imperative to mitigate the risk of unauthorized access and protect the privacy of the individuals using the app.

1.3 System Environment

A critical constraint embedded in the app's design is the incorporation of proper login and user data security measures. This constraint is paramount to safeguarding the privacy and confidentiality of the monitored individual's data. The app must implement robust authentication mechanisms to ensure that only authorized users can access sensitive information related to phone unlock activity. Additionally, user data, including personal information and monitoring logs, must be securely stored and transmitted. Adhering to industry best practices and data protection regulations is imperative to mitigate the risk of unauthorized access and protect the privacy of the individuals using the app.

2. Architecture

2.1 Overview

- **User Interface (UI):**

  The front-end component provides a user-friendly interface for both the isolated individual and caregivers. It displays relevant information, such as phone unlock activity, alerts, and emergency contact details.

- **Mobile Application:**

  The core of the system is a mobile application installed on the user's smartphone. The app continuously monitors phone unlock activity and sends encrypted data to the server for analysis.

- **Data Collection:**

  The app collects phone unlock data, including timestamps and patterns. This information is securely transmitted to the server for further processing.

- **Server-Side Processing:**

  The server-side component is responsible for receiving, processing, and analyzing the collected data. It employs algorithms to detect patterns indicative of prolonged inactivity or sudden falls.

- **Alert Generation:**

  When the server identifies concerning patterns, it triggers the generation of alerts. These alerts may include notifications within the app, messages to emergency contacts, and, if necessary, communication with external emergency services.

- **Customizable Settings:**

  The app allows users and caregivers to customize alert thresholds and notification preferences based on individual needs. This ensures a personalized and adaptive monitoring experience.

- **Privacy Controls:**

  Robust privacy controls are integrated into the architecture, emphasizing user consent, data encryption, and adherence to relevant privacy regulations. The system is designed to prioritize the confidentiality of user information.

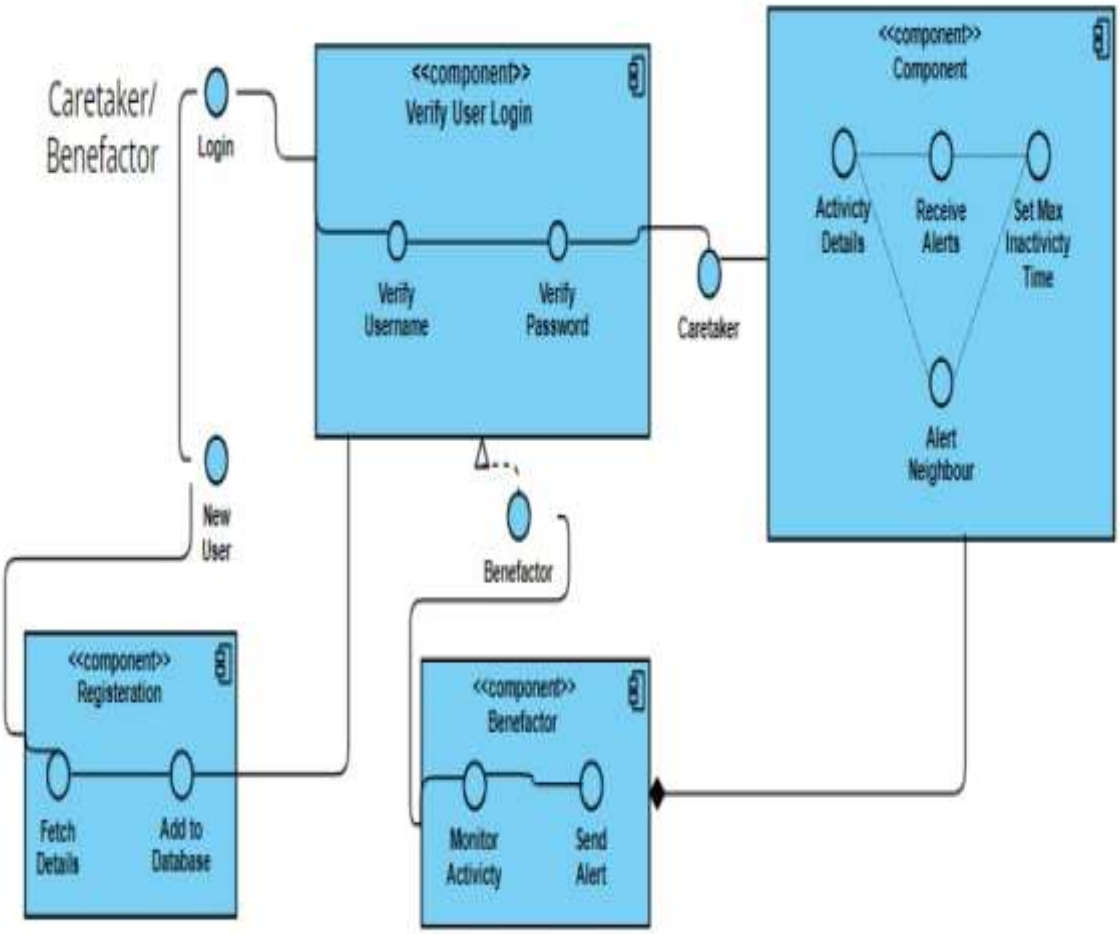
- **Emergency Response Integration:**

  The app may integrate with emergency response services, allowing for seamless communication and coordination in case of a detected emergency. This ensures a rapid and efficient response to critical situations.

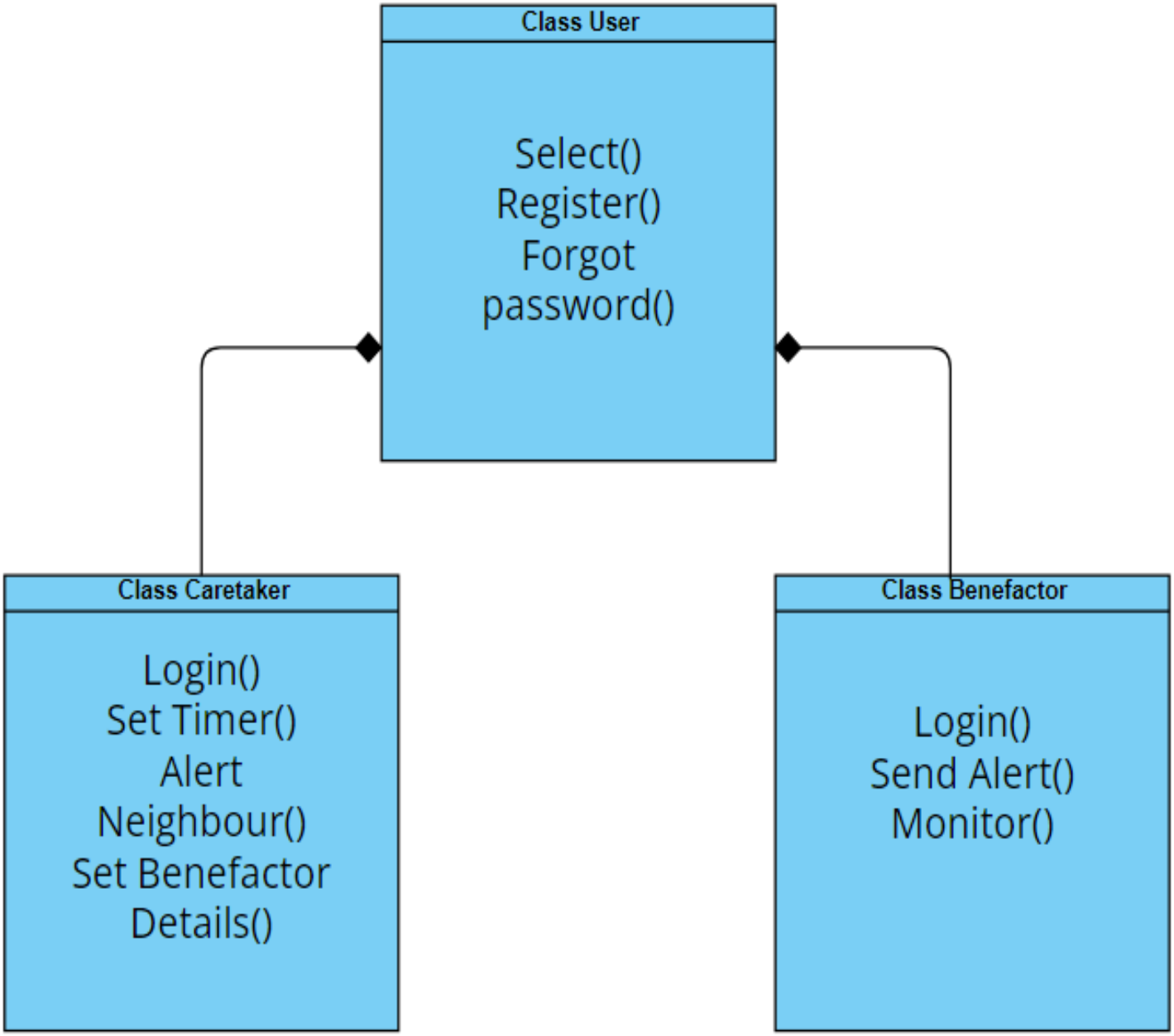
- **Secure Data Storage:**

  The architecture includes secure data storage practices, employing encryption techniques to safeguard user information. Compliance with data protection regulations is a crucial aspect of the system's design.

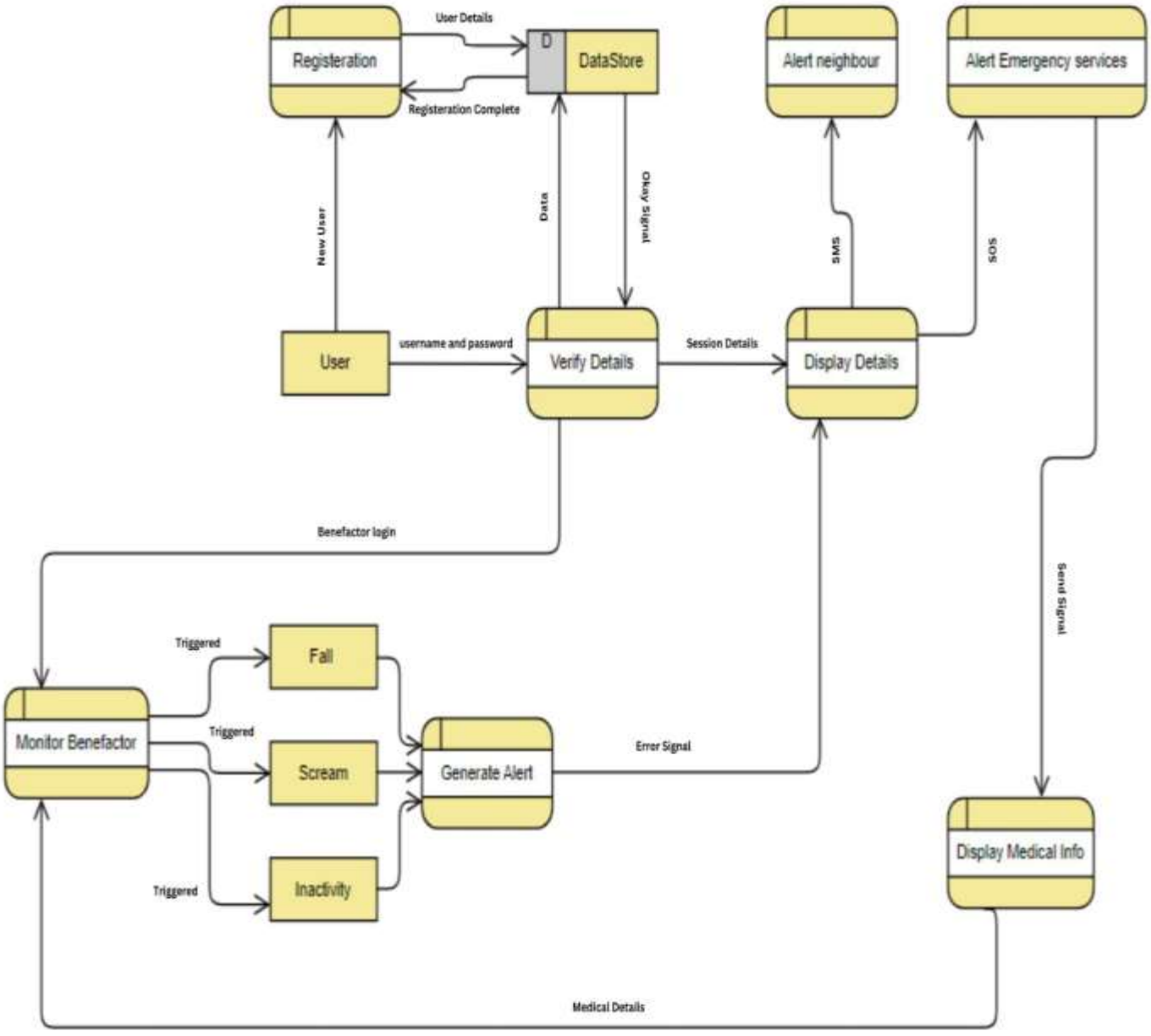
2.2 Component Diagrams



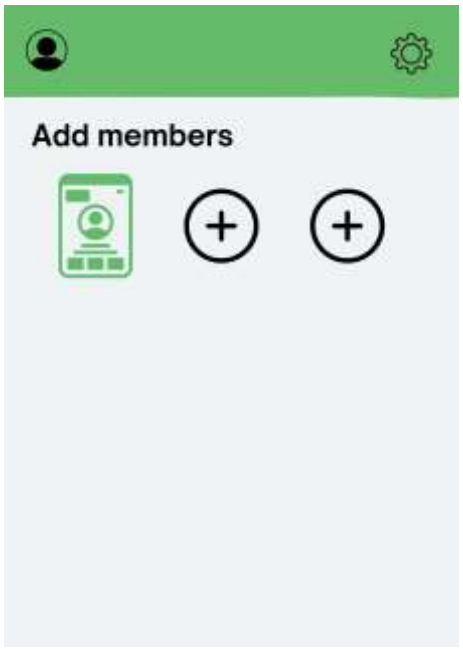
2.3 Class Diagrams

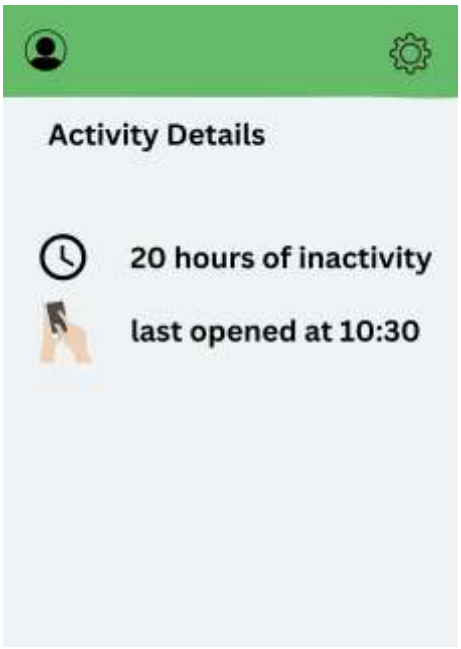


2.4. Data Flow Diagram

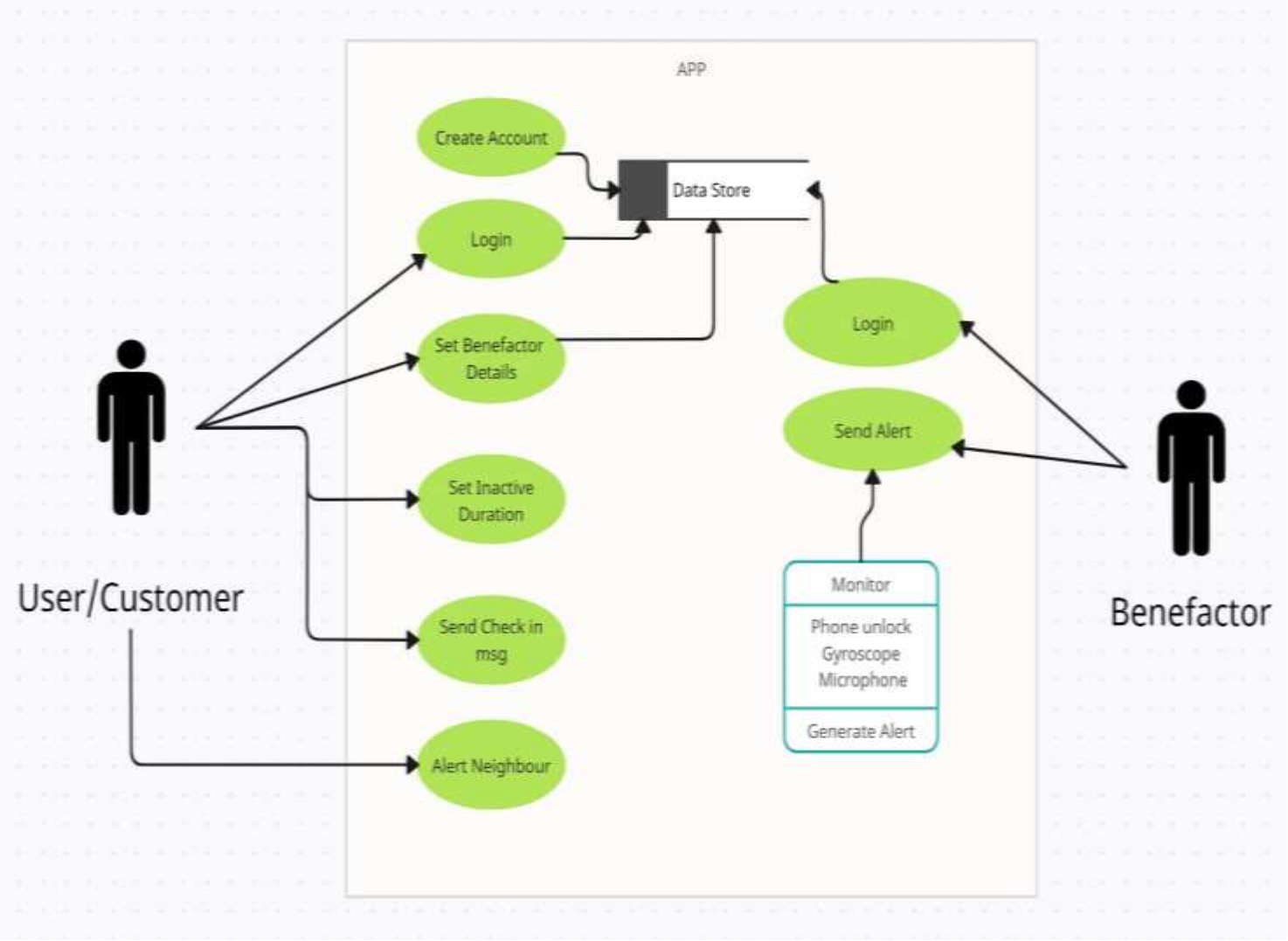


3. User Interface Design





4. Use Case Diagram



Appendix A: Team members

1	Sai Anand K	-	20221074
2	Shiva Surendran	-	20221076
3	Sidharth Thejas	-	20221079
4	S R Angleo Antony	-	20221081