**IMPLEMENTATION**

**MODULES:**

* Patient
* Doctor
* Cloud Server
* Data collection and encryption phase
* Data retrieval phase
* Conditional authorization

**MODULES DESCSRIPTION:**

**Patient**

In the first module, we develop the Patient module where the new patient is registered by entering their details in the registration form. Once after registration the patient cannot able to login in to the system. Only if the cloud server approves the patient only they can login into the system, this is developed to avoid unnecessary users and act as a security layer for the system. This module is responsible for managing patients' personal healthcare records (PHRs) and providing access the data uploaded by the patient. It collects the PHRs from various devices, encrypts them, and uploads them to the cloud server for secure storage. In the patient module, the patient should upload their details with Blood Group, Temperature, Blood Pressure etc. Each patient is created with Unique Patient ID to avoid duplications.

**Doctor**

In this module, we develop the Doctor’s part, where the new doctor is registered by entering their details in the registration form. Once after registration the doctor cannot able to login in to the system similar to the earlier module. Only if the cloud server approves the doctor only they can login into the system, this is developed to make the system more secure. The doctor module provides authorized doctors with access to patients' PHRs. It allows them to search for patients available securely and ensure the confidentiality of the PHRs.

**Cloud Server**

The cloud server module acts as an intermediary between the patient and doctor modules. It stores the encrypted PHRs and handles requests for data retrieval. We have used DriveHQ cloud service provider for the storage of files in the cloud part. In this module cloud server is built with the responsible to approving or rejecting both the patients and doctors also to make the system secure. The Cloud server is responsible for assigning a patient to the doctor. Also if any doctor requests for a particular patient, then the cloud server verifies and approves it accordingly.

**Data collection and encryption phase**

This module is responsible for collecting patients' PHRs from various patients and encrypting them before uploading them to the cloud server. It also ensures the confidentiality, integrity, and availability of the PHRs by implementing security protocols.

**Data retrieval phase**

The data retrieval module is responsible for handling authorized doctors' requests for medical records. It retrieves the relevant data from the cloud server, decrypts it, and returns it to the doctor module. Only if the particular decryption key is available they can able to access the data orelse the data cannot be accessed. The key will not be same for all the entity for the same file. So even if one entity leaks the key the file is still secure and cannot be accessed.

**Conditional authorization**

This module is the core of the DSAS project, which provides a secure and practical proxy searchable re-encryption scheme for efficient and safe remote PHRs monitoring and research. It allows Alice (doctor-in-charge) to delegate medical research and utilization to Bob (doctor-in-agent) through the cloud server, supporting minimizing information exposure to the cloud server.