**Abstract**

Cloud computing is an Internet-based computing pattern through which shared resources are provided to devices on demand. With integrating into cloud computing, security issues such as data confidentiality and user authority may arise in the mobile cloud computing system, and it is concerned as the main constraints to the developments of mobile cloud computing. In order to provide safe and secure operation, a hierarchical access control method using modified hierarchical attribute-based encryption (M-HABE) and a modified three-layer structure is proposed in this project. This project focuses on protecting the hospital data’s in a secure manner, the data can be sensitive to unauthorized third party and constraint to legal users as well. The novel scheme mainly focuses on the data processing, storing and accessing, which is designed to ensure the users with legal authorities to get corresponding classified data and to restrict illegal users and unauthorized legal users get access to the data, which makes it extremely suitable for the mobile cloud computing paradigms. In this project the key authority will generate the key to the requested data owner (Nurse, doctor and admin). The keys are generated under three authorities with three different attributes. Using the key the data owner will encrypt the file and add them in the website. If the user wishes to see their data’s then by using the key the user can view their data’s. The key is provided based on the patient ID and selected dataset entered by the user. If the details is matched then the user can get the key from the data owner, using the key the user can view their needed data through this website.

**Front End:** JAVA

**Back End:** My SQL

**MODULES**

The module used in this project are,

* Key authentication
* Data owner
  + Nurse
  + Doctor
  + Admin
* Data user

**Key authentication**

Key authenticator plays the major role for key generation. The key authenticator login into the system using their login credentials. After login the key authenticator will view the key request. The keys are generated based on the key authority chosen. In the key authentication center there are three authorities and each authority has a unique attributes. Based on the authority and attributes chosen the keys are generated. The generated key is distributed to the requested data owner.

**Data owner**

Data owner module contains three owners namely nurse, doctor and admin. The admin has the major role of uploading the data in the cloud. The nurse login into the system and enter the patient details in the website. The doctor login into the system using their login credentials, after login the doctor will view the entered patient details. After viewing the patient details, the doctor will provide treatment to the patient and add the medicine and test details in the website. The admin will login into the website and view the patient test and medicine details entered by the doctor and nurse. The admin will make request to the key authority. After getting the key the admin will encrypt the patient file using the key and upload the data’s in the cloud.

**Data user**

The data users are the patients. The data user who wants to view their data’s needs to login into the system. After login the data user needs to enter the patient ID and the type of dataset the user wishes to see. After entering the details if the entered data’s matches with the details in the database then the user is allowed to access the system. Then the user needs to get the key using the get key option. By entering the key the user can access the needed file from the cloud.