# *Two Layer Encryption for Data Security In Public Clouds*

Cloud computing is a rising computing technology. It permits users, store their data, knowledge or information remotely. The purpose of this paper is to secure access control scheme for public clouds. Here presents a "Two Layer Encryption for data security in Public Clouds", which provides more security and privacy. Data privacy and security issues have been major concerns for many organizations. Data often contains sensitive information and should be protected as mandated by various organizational policies and legal regulations. For this such organizations uses cloud computing for secure data storage and retrieval with the help of encryption. Encryption is a commonly adopted approach to assure data confidentiality.

In proposed system uses two layer encryption. The example hospital uses Two Layer Encryption. The hospital admin performs the first layer encryption and the second layer encryption is done in cloud .The hospital admin encrypt and stores patient's EHR into cloud and the employees download from cloud whenever they need and decrypt the EHR. With this technique the security of patient's information become more powerful than the existing system.The data owner and the cloud service utilize a broadcast key management scheme whereby the actual keys do not need to be distributed to the users. Instead, users are given one or more secrets which allow them to derive the actual symmetric keys for decrypting the data.

Administrator has full control of the system and admin act as the owner of this system. All the initial setting is done by the administrator. Admin can monitor all the activities of the user. The administrator is provided with admin id and password. Using which, the admin can enter into his part of the site. The job of the administrator is to add users at the hospital. The users are doctor, receptionist and patient. The patient is add by receptionist. The main role of admin is to encrypt the EHR (Electronic Health Record) using Advanced Encryption Standard (AES) algorithm and upload into public cloud.The Users in this system can login into the site using their username and password given by admin. The receptionist has the duty to add patient and assign doctor according to patient's EHR. The doctor download EHR from cloud and decrypt using AES algorithm. After that the doctor send the data to admin. The patient has the duty that they can view their profile and also view the doctor assigned by receptionist.In this module the users send the EHR to the admin and the admin encrypt the data using AES algorithm and upload into cloud. Then the cloud owner re-encrypt the EHR and stored into cloud. Users download encrypted data from the Cloud and decrypt to access the data. For decrypting users using the algorithm that is AES.