**PSMPA: Patient Self-controllable and Multi-level Privacy-preserving Cooperative Authentication in Distributed m-Healthcare Cloud Computing System**

**INTRODUCTION**

Data mining (sometimes called data or knowledge discovery) is the process of analyzing data from different perspectives and summarizing it into useful information - information that can be used to increase revenue, cuts costs, or both. Data mining software is one of a number of analytical tools for analyzing data. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases. Data mining is primarily used today by companies with a strong consumer focus - retail, financial, communication, and marketing organizations. It enables these companies to determine relationships among "internal" factors such as price, product positioning, or staff skills, and "external" factors such as economic indicators, competition, and customer demographics. And, it enables them to determine the impact on sales, customer satisfaction, and corporate profits. Finally, it enables them to "drill down" into summary information to view detail transactional data.

**SCOPE OF THE PROJECT**

The scope of our project a new technique of attribute-based designated verifier signature, a patient self controllable multi-level privacy-preserving cooperative authentication scheme realizing three levels of security and privacy requirement in distributed m-healthcare cloud computing system is proposed. By using model of key extraction algorithm which is used the directly authorized physicians, the indirectly authorized physicians and the unauthorized persons in medical consultation can respectively decipher the personal health information and/or verify patients’ identities by satisfying the access tree with their own attribute sets.

.

**MODULES**

* User Interface Design
* Key Generation Model
* Encryption and Decryption Model
* Prescription model

**MODULE DESCRIPTION**

User Interface Design:

To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id . Logging in is usually used to enter a specific page.

Key Generation Model:

In this model the key generated by using Anonymous Id Assignment technique for that users wants to sharing the data’s to database environment. Because the users upload the N no. of files can upload o the cloud with the ID assignment key only possible.

Encryption and Decryption Model:

In this model the users wants to upload the files among the database. if either public or private mode of users to shares to the cloud. Whenever the users to upload the files with the key only can upload else can’t. The files it could be either multimedia or any kind of files we can upload with the help of key. And the values finally converted into encryption model. After that the values are converted into decryption format.

Prescription Model:

In this model the physician prescribe the based on the problems and the physician will know about the patients details regarding the problems.

**MODULES DIAGRAM**

User Interface

Server

Database

Login Page

Patient

Key Generation Model

Login

Patient Registration

Re

Key Generator

Cloud

Encryption and Decryption Model

Patient Login

Patient Registration

Re

Key Generator

Files Encrypting

Cloud

Files Decrypting

Prescription Model

Decryption and Key

Cloud

Physician (or) Doctor

**INPUT EXPECTED OUTPUT:**

* Patient Interface Design

Input : Patient Login name and Password.

Output : If Valid Patient Open the window otherwise error page.

* Key Generation Model

Input : Automatic Symmetric key.

Output : It will generate random Symmetric key.

* Encryption and Decryption Model

Input : upload the patient’s attributes among the clod server.

Output : Patient attributes can upload and encryption otherwise error will occur.

* Prescription Model

Input : give the same Login Key.

Output : Physician can view the Patient’s files.

**SYSTEM REQUIREMENTS**

**HARDWARE**

PROCESSOR : PENTIUM IV 2.6 GHz, Intel Core 2 Duo.

RAM : 512 MB DD RAM

MONITOR : 15” COLOR

HARD DISK : 40 GB

**SOFTWARE**

Front End : Java (Jsp, Servlet)

Back End : MY SQL 5.5

Operating System : Windows 07

IDE : Eclipse

**Use Case Diagram:**

Patient

login

requests

Cloud server

get response

**EXPLANATION:**

The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted. In our use case diagram first user login into user window then if it is a valid user means then it can communicate with the cloud server. The major advantage of the thing is if client requests some data then the request will reach to the server then the data which is requested by the client is there with the cloud server then it will be processed and effectively sending data to the requested client. If the data is not there with the cloud server then it has to search in its related clients and if the resource is there means then it will be shared to the particular requester.

**Class Diagram:**

user



name



password



request response()



response()

login



name



password



submit()



reset()

client1



client ip address



server information

...



request()



response()



share()

cloud server



server ip address



index



request information



receiving requests()

...



process requests()



sending response()



...



**EXPLANATION:**

In our class diagram we having the details about user, if it is a valid user means then it can communicate with the cloud server. The major advantage of the thing is if client requests some data then the request will reach to the server then the data which is requested by the client is there with the cloud server then it will be processed and effectively sending data to the requested client. If the data is not there with the cloud server then it has to search in its related clients and if the resource is there means then it will be shared to the particular requester.

**Object Diagram:**

Cloud Server

**EXPLANATION:**

First Patient login into user window then if it is a valid user means then it can communicate with the cloud server. The major advantage of the thing is if client requests some data then the request will reach to the server then the data which is requested by the client is there with the cloud server then it will be processed and effectively sending data to the requested client. If the data is not there with the cloud server then it has to search in its related clients and if the resource is there means then it will be shared to the particular requester.

**State Diagram:**

User

Login

Upload & Encryption

Physician

Key

Cloud Server

**EXPLANATION:**

The major advantage of the thing is if client requests some data then the request will reach to the server then the data which is requested by the client is there with the cloud server then it will be processed and effectively sending data to the requested client. If the data is not there with the cloud server then it has to search in its related clients and if the resource is there means then it will be shared to the particular requester.

**Activity Diagram:**



**EXPLANATION:**

first user login into user window then if it is a valid user means then it can communicate with the cloud server. The major advantage of the thing is if client requests some data then the request will reach to the server then the data which is requested by the client is there with the cloud server then it will be processed and effectively sending data to the requested client. If the data is not there with the cloud server then it has to search in its related clients and if the resource is there means then it will be shared to the particular requester.

**Sequence Diagram:**

patient

Login

Upload

Key

Physician

user logins

Datas upload to server

requests resource

get key

Key Accessing

attributes

**EXPLANATION:**

In our sequence diagram specifying processes operate with one another and in order. In this first user login into user window then if it is a valid user means then it can communicate with the cloud server. The major advantage of the thing is if client requests some data then the request will reach to the server then the data which is requested by the client is there with the cloud server then it will be processed and effectively sending data to the requested client. If the data is not there with the cloud server then it has to search in its related clients and if the resource is there means then it will be shared to the particular requester.

**Collaboration Diagram:**

Patients

Login

Server

Physician

1: user logins

2: connects to server

3: upload data+Symmetric key

4: get symmetric key

5:Download

**EXPLANATION:**

A collaboration diagram describes interactions among objects in terms of sequenced messages. Collaboration diagrams represent a combination of information taken from class, sequence, and use case diagrams describing both the static structure and dynamic behavior of a system. In this a user login into user window then if it is a valid user means then it can communicate with the cloud server. The major advantage of the thing is if client requests some data then the request will reach to the server then the data which is requested by the client is there with the cloud server then it will be processed and effectively sending data to the requested client. If the data is not there with the cloud server then it has to search in its related clients and if the resource is there means then it will be shared to the particular requester.

**Data Flow Diagram:**

**Level-0:**

Data Base

Symmetric key & Physician

Error Page

**EXPLANATION:**

It does not show information about the timing of processes, or information about whether processes will operate in sequence or in parallel. In the DFDs the first user login into user window then if it is a valid user means then it can communicate with the cloud server. The major advantage of the thing is if client requests some data then the request will reach to the server then the data which is requested by the client is there with the cloud server then it will be processed and effectively sending data to the requested client. If the data is not there with the cloud server then it has to search in its related clients and if the resource is there means then it will be shared to the particular requester.

**E-R Diagram:**

Patient

Symmetric Key

Cloud Server

Symmetric Key

Physician

**EXPLANATION:**

Entity-Relationship Model (ERM) is an abstract and conceptual representation of data. Entity-relationship modeling is a database modeling method, used to produce a type of conceptual schema or semantic data model of a system, often a relational database. In our ER diagram the client is there with the cloud server then it will be processed and effectively sending data to the requested client. If the data is not there with the cloud server then it has to search in its related clients and if the resource is there means then it will be shared to the particular requester.

**Component Diagram:**

Patient

login

File

Upload

a

Physician

Cloud server

File download

**EXPLANATION:**

In the Unified Modeling Language, a component diagram depicts how components are wired together to form larger components and they are used to illustrate the structure of arbitrarily complex systems. For this in our component diagram we did the first user login into user window then if it is a valid user means then it can communicate with the cloud server. The major advantage of the thing is if client requests some data then the request will reach to the server then the data which is requested by the client is there with the cloud server then it will be processed and effectively sending data to the requested client. If the data is not there with the cloud server then it has to search in its related clients and if the resource is there means then it will be shared to the particular requester.

**Future Enhancement:**

The extension of the proposed main scheme the formal security proof and efficiency evaluations which illustrate various kinds of malicious attacks and far outperforms previous schemes in terms of storage, computational and communication overhead. In our project we are going to do the patient attribute values are stored in among cloud server only based on the patient problem not for maintained every patient. The separated data base we are allocated to every problem. So, that easily to achieve the data mining concept. The patient value must be an encrypted, the encrypted data’s are stored among the cloud Server. The time of entering the patient must and should login then only permit to allow the take all attribute tests. So the login and the encrypted values to be decrypted by the same key only access. So the contacting key must by the way of contacting mail only. And also the patient attribute test compared with patient problem values, so easily to identify the problem and prescription also made easily by the doctors.

**ADVANTAGES:**

* To achieve more Secure and Privacy.
* The patient’s attributes are encrypted.

**CONCLUSION:**

A new model authorized accessible privacy model and a patient self-controllable multi-level privacy preserving cooperative authentication scheme (PSMPA) realizing three different levels of security and privacy requirement in the distributed m-healthcare cloud computing system are proposed.