Secure Sharing of Health Records in Cloud

THESIS SUBMITTED IN PARTIAL FULFILMENT OF REQUIREMENT
FOR THE AWARD OF THE DEGREE OF

Master of Technology
in
Software Engineering

Under the guidance of
Mr. Manoj Kumar
(Associate Professor H.O.D, Computer Center)
Delhi Technological University

Submitted By -
Sohit Rajput
(Roll No. 2K17/SWE/17)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)
Shahabad Daulatpur, Main Bawana Road, Delhi-110042

June 2019

DECLARATION

I hereby declare that the thesis work entitled "**Secure Sharing Of Personal Health Records in Cloud Based Architecutre**" which is being submitted to Delhi Technological University, in partial fulfilment of requirements for the award of degree of Master of Technology (Software Engineering) is a bonafide report of Major Project-II carried out by me. The material contained in the report has not been submitted to any university or institution for the award of any degree.

Place: Delhi

Date:

Sohit Rajput

Roll No. 2K17/SWE/17

CERTIFICATE

This is to certify that Project Report entitled "**Secure Sharing Of Personal Health Records in Cloud Based Architecutre**" submitted by Sohit Rajput(roll no. 2K17/SWE/17) in partial fulfilment of the requirement for the award of degree Master of Technology (Software Engineering) is a record of the original work carried out by him under my supervision.

Place: Delhi

Date:

SUPERVISOR

Mr. Manoj Kumar

Associate Professor

Head Computer Center

Delhi Technological University

Bawana Road, Delhi -110042

ACKNOWLEDGEMENT

I am very thankful to **Mr. Manoj Kumar**(Associate Professor, Head of Computer Center) and all the faculty members of the Computer Science and Engineering Department of Delhi Technological University. They all provided us with immense support and guidance for the project.

I would also like to express my gratitude to the university for providing us with the laboratories, infrastructure, testing facilities and environment which allowed us to work without any obstructions.

I would also like to appreciate the support provided to us by our lab assistants, seniors and our peer group who aided us with all the knowledge they had regarding various topics.

SOHIT RAJPUT

Roll No. 2K17/SWE/17

M. Tech. (Software Engineering)

Delhi Technological University

ABSTRACT

Now a days the information technology is growing exponentially not only in the field of business and education its gaining its importance even in the field of the healthcare it has now become a common practice to send patients data over distances through internet. Thus in the field of the Healthcare we need to adopt the secure Personal Health Care Records(PHRs) generally the PHRs contain all the information of the patient such as personal and medical information in a digital format. Transmission of such important information over the internet is always susceptible to get hack thus it's of utter importance to provide such an architecture to our network so that it becomes prone to attacks.

In our report we will show our proposed architecture will be useful for securely transferring the personal health records. We will also explain various ways through which we can implement security in cloud-based architectures. We will analyze the advantages and disadvantages of various techniques that will be used to implement security. After the analysis of various techniques, we will explain the techniques that we will be using in our project. We explain and implement the described architecture and will study the performance evaluation of our project.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

1. CC	Cloud Computing
2. MCC	Mobile Cloud Computing
3. PHR	Personal Health Records
4. CDS	Cloud Data Server
5. MHT	Merkel Hash Table
6. E	Encrypt
7. D	Decrypt
8. SRS	Secure Re-Encryption Server
9. ABE	Attribute Based Encryption
10. DES	Data Encryption Standard

Chapter 1

Introduction

1.1 Basic Overview

Cloud computing framework turns out to be more famous which enables clients to access and concentrate on the delicate data at what point they require. This is basically appropriate in medicinal field, where the patient's individual Personal Health Records are frequently stored on outside server, for example, cloud suppliers. At the point when the Personal Health Records are put away and got to through the intermediary server, security turns into the primary concerns. The fundamental objective of this framework is to secure patient's Health care data information secrecy and only after the patients consent the outer elements, for example, specialists and medical attendants can access the patient's information. Hospitals are now considering that sharing information of patient over the cloud givers better and safe treatments to the patients. It's of no good use that each time a patient goes to some other doctor same tests need to be done through the health records maintained on the cloud doctor can easily see the entire history of all the treatments and procedures through which the patient has gone through. The proposed approach not only makes data easily available it also ensures the proper security concerns by encrypting the patient's data and only the authorized user could see the decrypted data.

Now a day's during the worldwide monetary downturn, exponential growth of organizations and internet business profoundly requires better and imaginative procedures for their development and expansion. Various developments over the time in area of Cloud Computing have reshaped procedures that define the Structure and growth of IT hardware. Cloud computing has been broadly perceived as the cutting-edge technology of present and future.

The cloud computing provides substantial potential to rise coordination among several Health care stake holders and also ensures nonstop availability of health information and scalability. Cloud computing proved to be platform for the next generation health records where data accessibility is more easily available, more securable and could be retained for years without loss of data.

What actually cloud computing conveys is a model that has capability to process information,storage and all the physical resources are provided to client on demand so client does not need to purchase costly hardware devices like servers, hard disks or any other network related equipment. Rather than purchasing genuine physical hardware equipment, storage servers or any systems administration hardware, customers can rent these things from a cloud supplier as redistributed administration.

Cloud Computing empowers clients to flexibly use assets in an on-request style. Today, the utilization of Mobile Devices is expanding step by step. Everybody has a cell phone which gives the office to move anyplace and get to the information whenever required. The expanding utilization of cell phones gave rise to Mobile Cloud Computing (MCC). MCC is the like combination between web and cloud computing. MCC gives new sort of the administrations to versatile clients to completely use the upsides of Cloud Computing.

Cloud Computing alludes to a framework where data processing and storage can occur not in mobile device but Device such as servers. Thing is Mobile devices does not need to have an over powered CPU and large storage capability since data processing is being placed outside the devices on a centralize server which is located may be at a distant location or we can say in Cloud.

Cloud computing could provide a model through which important entities of healthcare such as patients, Hospital Staff including doctors and nursing staff, pharmacy staff, laboratory personnel and any other related person could integrate.

Generally, the PHR contains personal information, health records such as allergies, past surgeries and treatments, laboratory reports, data about health insurance claims, current health conditions. PHR are maintained through the Internet based tools that allows

patients to create and manage health records and can be provided with the consent of the patient to all those who need to view and modify the records.

There are various factors which impose limitation on cloud based PHRs poor computation power, security factors, unreliable internet connectivity. Among all concerns Data security is most prominent one because of which most of users are not ready to take interest in Cloud based PHRs. Since data is being stored at a far location from the user so there is always security concern.

1.2 Definition of cloud and PHR

Cloud computing deals with providing computation as a part of service not as a whole product where resources are being shared such as software and hardware resources.

In cloud computing users are provided with computations, software accesses, data access and storage capabilities without knowing where does actual resources are located. End users could access cloud based applications through web browsers or other mobile applications while the actual location of application is unknown to the end user.

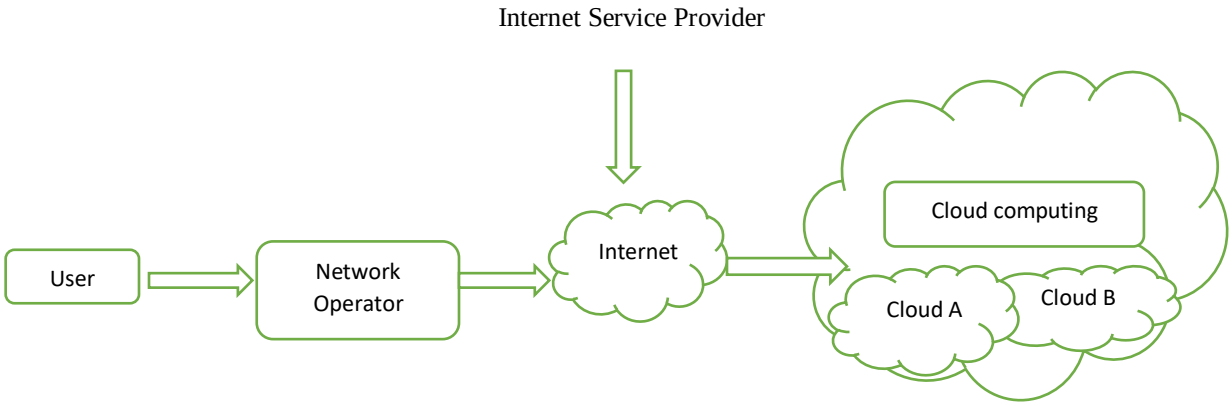

Fig 1.1 Cloud Architecture Diagram

Basically we can say assume cloud computing as a kind of service that allows users to changedata processing and information storage abilitiesbydividing and

loadingcomputationally concentrated and storage demands on cloud servers through wireless network access.

Whereas some organizations like Google concludes cloud computing as an emerging paradigm in the field of mobile applications in which almost Every kind of data processing and storage is transferred from the device to central computing platforms which are situated somewhere in cloud.

Electronic Personal Health Records

An electronic personal health record (EHR) is a kind ofdigital group of patient datastored in a digital format. The need of electronic health record is that they canenabledistribution of patient personal as well as healthcare data such as remedialhistory, charts, prescriptions and test results among multiple healthcare environments.

A personal health record (PHR) can be used by patients in order to collect, manage, and share all current and previous medical information. This can be in comparison to a medical health record which is generallycreated and maintained by a health care system, institution or government payer.

The one of foremost importance of PHR advantage is better patient access to a variedrange of trustworthy health data, data, and knowledge. Patients caneasily force that access to advance their health and manage their diseases. Using this information we can modify our PHR to make it more beneficial.

As self-monitoring technologies, have become more accessible and affordable, healthcare technologists have started to use tools like the personal health records (PHRs) to enable patients to be more connected with their health data. PHRs are technology applications that create a private and secure environment for users to access, manage and share their medical data. PHRs are essential for allowing patients to control their healthcare information and for acting as an engagement tool with their health practitioners. The primary consumers of PHRs are patients. The goal of a PHR is to empower patient participation in their care by conducting their health info and to improve communication among the patient and their providers

1.3. Advantages and Disadvantages of PHRs

There are numerous benefitsof maintaining an ePHR. To start with the use of ePHRa patient can easily access his details from anywhere and anytime in the world with the use of any web-enabled deviceat any time. Patients can manage their ePHR through phones, tablets, desktops or laptops they just need a internet connection. And during emergency conditions it is very useful to have your medical history in hand. If you have all the records stored in an electric format then it is much easier to share your medical history including medications, allergies and chronic conditions, with the emergency personnel. It is also useful if you plan to track your health records or if you want to check your health progress between your clinical visits. With the help of ePHR it would become very easy to make notes from doctors' advice.Medical equipment that are used to check your heart beat rate, sugar leveletc. can also be modified so that entire details get automatically uploaded to your PHR.Patients then can evaluate their health conditions. Having all medical history at one place is important you do not need to scroll through multiple files to check your history.

Some of the basic advantages:

Easier Understandability and Readability: This can easily be said that electronicrecords are far easier to read than medical doctor hand written notes.Through this there is no case of understanding and even a common man can also read reports.

Simplicity and Time saving: With the use of PHRs you don't need to waste time scrolling through paper records. You can simply search your desired record just by going through web portal.

Space Management: By the support of ePHR now hospitals don't require any physical space to store bulky files they just need space enough to place a desktop, laptop or even a tablet or mobile phone.

Patient Accessibility: ePHR allows patients to view their medical records such as previous and current medical conditions, they also shows what is the current treatment they are going through and what medications they are taking.

Financial Incentives: Government of INDIA is also promoting digital India thus ePHR is step towards fulfilling that dream in these cases Government of India also provides financial aids so that you can implement in ePHR.

Even though there are a lot of benefits to an ePHR, still there are some risk and drawbacks. Like, it is difficult and consumes a lot of time to collect current as well asearlierremedial information. Patients need permission from different medical healthcare centers and pharmacies in order to get entire medical information. Some of the material such as immunization records may date back to juvenile and it becomes difficult to recall that information. To store all medical information at one place is difficult because most of the time patients to don't know from where to start.

1. **Privacy and Security Issue:** security and privacy is an important concern as every computer connected via network is prone to hacking. So its dangerous if your personal information gets to an unauthorized person.
2. **Information Update:** Since Electronic Health Records defines the health of a person at a particular instant it's very important to update these records after every clinical visit. If information is not updated then it means that other healthcare personnel will determine your health treatment by looking and outdated health record.
3. **Patient anxiousness:** since patients can contact their remedial data it can lead to a situation somewhere when they misunderstood any information and stared to fell panic.
4. **Reliability Concerns:** PHR becomes unreliable if there is any kind of error during transfer of records from paper to PHR system. This could result into wrong treatment practices.Doctors proceed their treatments only after looking at PHRs they should be held responsible if they don't go through entire information.

1.4 Problem statement: Secure Sharing of EPHR in cloud based Architecture

One of the important aspects of EPHR is securing the data of PHR owners. The files that contain all the information of patientsare very important and anyone who is unauthorized to see information may change the data in order to harm the user. That's why the main fear of to everybody is to offer the security where the data files are stored, created and updated time to time. The security of the data is very important for the user as it contains his/her confidential details. So it's very important that we should adopt a secured architecture for maintaining PHRs.

A Risk Model shown is shown below in Fig 1.2At this point User uses devices to upload PHRs and cloud administrator manages the cloud. The hacker may attack at the device and the cloud server he can also attack at the time when data transmission between the cloud and device will be taking place.

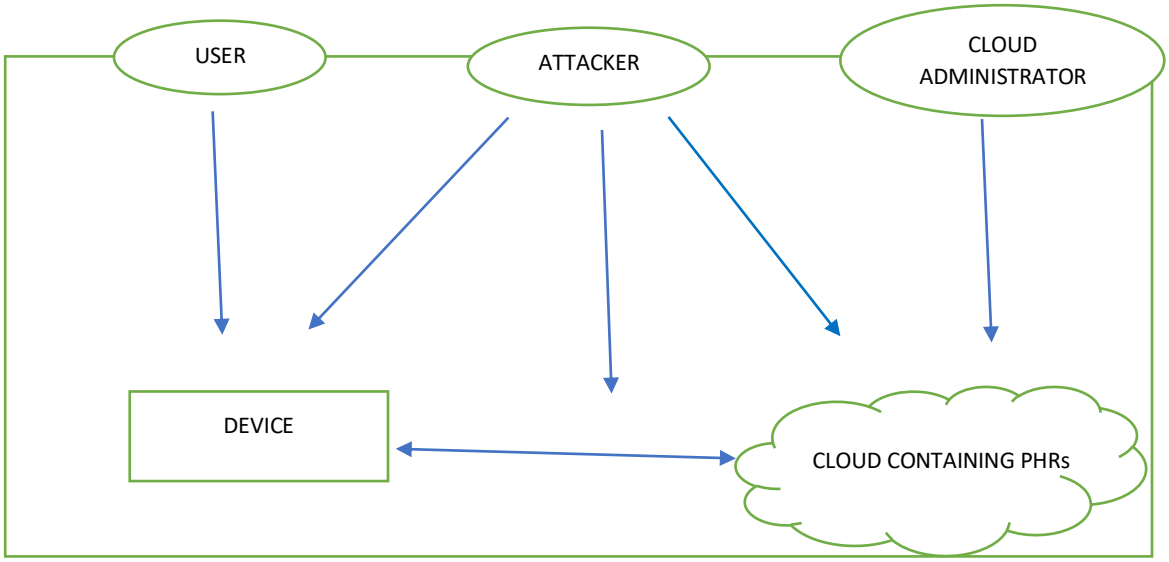

Fig 1.2 Risk Model in cloud based PHR

The attacker may attack at the PHR stored at the servers. For proprietor the confidentiality of the PHR is very vital. If in the least anunlicensed person makes some changes in the data then the truthfulness of the data is lost. Any person if get know the PHR of the user he may harm the user in many ways. The confidentiality of the data is prime concern in these kinds of architecture.

Table 1.1 Different kinds of security threats:

Attack	Description
Viruses and Worms	These are the piece of codes used to degrade the performance of the computer.
Rouge Security Software	Misleads user in believing there is virus in computer and forces to download their program that leads to real malware being upload on the computer
Adware and Spyware	Contains key loggers that record personal information like transaction ids and passwords.
DOS and DDOS Attack	Performs overloading of traffic on a network so that legitimate users will unable to use it.
Rootkit	Enables remote control and administration level control at computers or network. After remote access attacker may steal passwords, disable antivirus etc.
SQL Injection attack	They target data driven applications they uses malicious code that may obtain private data, change data, can vanish data.
Man in Middle Attack	Attacker targets the network that is established between two persons and steals information. Eg: DNS spoofing, IP spoofing

1.5 Objective:

The given research work is provided with the following given objectives:

1. To study the existing methods of storing PHRs along with various problems that they faces.
2. To provide a new method for storing PHRs in cloud-based architecture.
3. To analyze proposed mechanism.

1.6 Motivation

As self-monitoring technologies have become more accessible and affordable, healthcare technologists have started to use tools like the personal health records (PHRs) to help patients become more connected with their health data. PHRs are technology applications that create a private and secure environment for users to access, manage and share their medical data. PHRs are essential to allowing patients to control their healthcare information and to act as an engagement tool with their health practitioners. The aim of a PHR is to enable patient's contribution in their care by conducting their health information and to advance faster and better communication among the patient and their providers.

There are numerous benefits when a patient has access to important health information in his/her personal medical record.

Patient Engagement:

Patient involvement in their health care primarily takes place outside of the hospital setting. Therefore, if patients are provided with the appropriate tools to track their progress and manage their care, their engagement within their own care process increases.

Patient-Provider Communication:

Patient health records facilitate a direct line of communication between patients and their providers. When communication is easier (more direct as well as faster) patients constantly provide their feedback, which helps providers intervene earlier and improve

the care management process. All these interactions can be directly integrated into the patient's chart.

Patient use of their personal health records facilitates an exchange of information similar to that of a physical appointment; just like as an extension of the medical visit. Through the patient portals, patients can complete the following things themselves online:

1. Can check and schedule their appointment they can also schedule appointment.
2. Go through lab reports and also see basic patients' information like BMI, sugar level, weight and BP.
3. Examine medical statements and also medical charges.
4. Can request for the prescription.
5. Fill new patient forms and registration information.
6. Correspond with medical personnel via encrypted email services

All of these functions benefit both patients as well as providers; personal health records could help them stay well connected and well informed during the care process.

1.7Thesis Outline:

In this chapter introduction to the secure transmission of PHR data in cloud based architecture is highlighted. In the section 1.1 we have given the basic overview of the cloud based architectures and what exactly are PHRs we have also discussed the some of the basic implementations in this section. In the section 1.2 we have given some basic definitions of the cloud architecture and PHRs and also have tried to highlight some of the basic issues in the cloud based PHRs. In the section 1.3 we have discussed some of the basic advantages and disadvantages of using the PHRs. In the section 1.4 we have mentioned our problem statement and defined what we are going to do to solve that problem we also have presented some of the basic risk model in current designs and also presented the treats and vulnerabilities to the current architecture. In the section 1.5 we have presented the objective of our work mentioned the causes which forced us to do this report. In the section 1.6 we have defined our motivation towards the work.

Chapter 2 provided us with the overview of the related work in the field of the cloud based PHRs. Section 2.1 introduces the cloud computing in the section 2.2 we have shown the cloud computing architecture in the section 2.3 we have shown the general architecture of cloud based PHRs. In the section 2.3 we have discussed the various applications of the phr. In the section 2.4 we have mentioned the advantages of PHRs. In the section 2.5 we have presented the literature survey that we have performed before preceding our work.

Chapter 3 provides us with the various techniques that has been used till now to make secure access of PHRs. In the section 3.1 we have discussed the current work going on in the field of the privacy protection. Inside the section 3.2 we will discuss the present work going on in the area of the storage security. In the section 3.3 we will discuss the current work in the field of the data integrity. In the section 3.4 we will discuss about the current work going on in the field of the Access Control. In the section 3.5 we have mentioned work in the field of Attribute Based Encryption. In this section we have also presented a table to compare the existing schemes. In the section 3.6 we have discussed the techniques that are being used in existing schemes.

Chapter 4 will discuss the proposed solution in this chapter we have shown the working of our solution and the techniques that we have adopted. Inside the chapter 4.1 we have mentioned the architecture of the proposed solution. In the chapter 4.2 we have shown the working of the proposed solution.

Chapter 5 we will perform some analysis of our work. Section 5.1 will discuss about the security analysis whereas the chapter 5.2 will discuss about the performance analysis.

In chapter 6 we have shown some of the experimental results of our works and in the chapter 7 we have discussed about the future work that could be done in this field.

Chapter 2

Literature Survey

2.1 Cloud Computing

Cloud computing is a prototype of internet-based computing which assist shared computers processing resources and data to computers and other devices on request. It is also used for enabling resource presents, on demand access for example computer networks, servers, storage, applications and services.Data de-duplication is a process that removes repeated copies of data and reduces storage overhead.

National Institute of Standards and Research gaveworldwide accepted definition of cloud computing as:

"Cloud Computing is a model of enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management efforts or service provider interactions. This cloud model promotes availability and is composed of five essential characteristics, three service models and four development models."

Now Cloud computing is developing innovation in the area of data circulation. Cloud computing is utilization of resource (software and hardware) that can be provided as a service through a network just like internet. Pretty much Cloud computing depicts exceedingly versatile resources provided as an external service through web on pay-as-ease of use premise. The term cloud computing instigates from the cloud formed image which is utilized to show a distant asset associated by means of the web.

Cloud computing may be described as: In case of water supply user can merely use it. They do not requireworrying from where the water is coming, how it is purified, or how

it is supplied. In the end of the month users will get the bill for the volume of water they have consumed. Cloud computing also works on the similar idea, the users can simply use the resources such as computing powers, storage capabilities without worrying how these things works internally. The basic clue behind cloud computing is that handlerneeded to pay only for those things which they truly use.

The elementaryadvantages of the cloud computing over the traditional one are that they can be used to provide infrastructure to users such as Networks, storages, servers. They can also be used to provide the platforms such as middleware services and operating systems along with them they are used to provide software such as application programs. The cloud can provide a remote architecture in which a user can access services, data and applications remotely. In this situation user require to pay only for those things which he really wants to use.

2.2 Cloud Architecture:

The basic services of a cloud are defined as a layered concept. In which every layer has its separate functionality. A Cloud Architecture is shown in Fig.2.1. It has 3 layers:

1. Data center layer: At this layer various services are connected to each other with the help of high-speedwebs in order to run services to the customer.

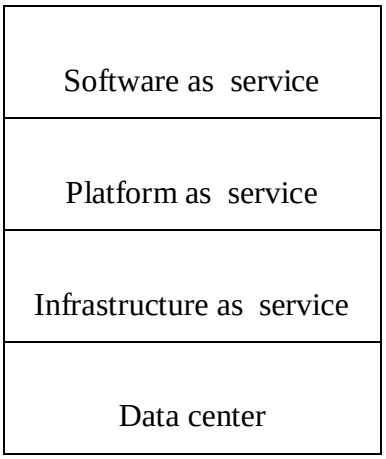

Fig: 2.1 Service oriented Cloud Architecture

2. Infrastructure as a Service (IaaS): It provides the facility to storage, servers, hardware and networking equipment. Through this the user need to pay per use basis. Examplesare Simple Storage Services and Amazon Elastic Cloud Computing.
3. Platform as a Service (PaaS): It offers an innovativeunified environment through which we can build tests and install our traditional applications. The examples of PaaS are Microsoft Azure,Google App Engine and Amazon Map Reduce/Simple Storage Service.
4. Software as a Service (SaaS): It provides the software distribution by meeting some specific requirement criteria. With the help of this layer a user can contact applications and information distantly through the use of internet. Salesforce is among the best in giving this service model.

2.3General Architecture of Cloud Based PHRs

General Architecture of Cloud based PHRs is shown in the figure 2.2 given below which shows the connection between the PHR owner, application server and PHR users.

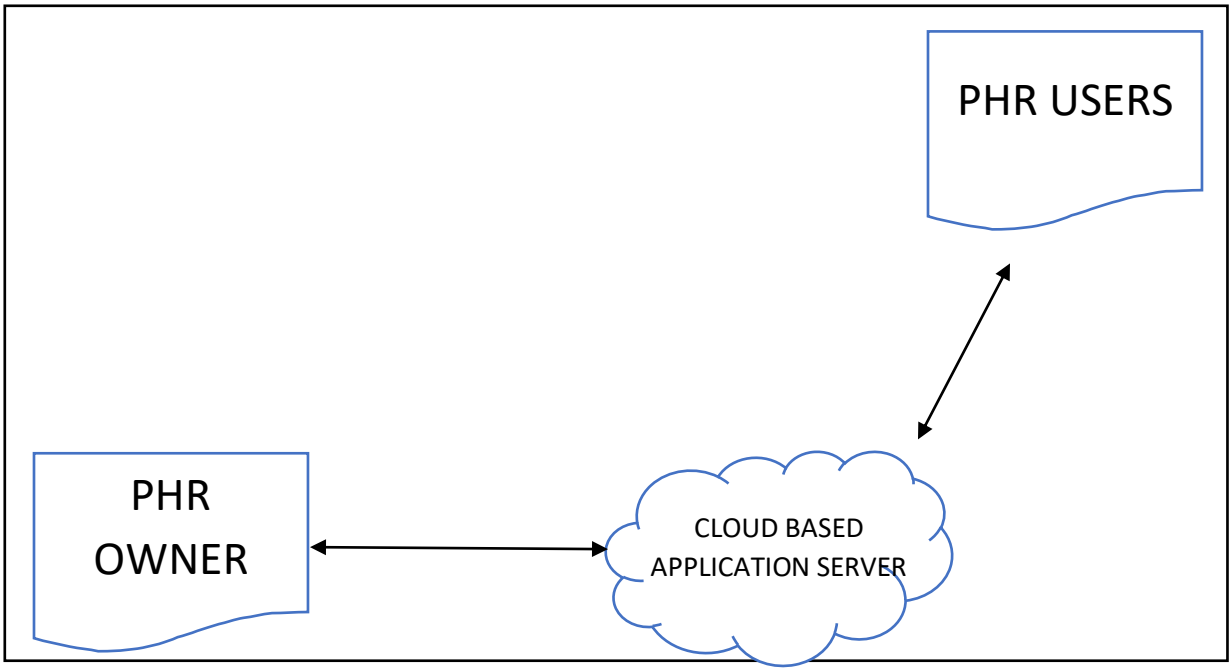

Fig: 2.2 General Architecture of cloud based PHR

1. PHR Owner: PHR owner is the one whose information gets uploaded to the application server. He is the one who came for the diagnosis. Owner of the PHR can upload their information such as its personal details such as Name, Address, and Telephone number etc. other information such as medical history, insurance related information and prescription information is also uploaded by the PHR owner.
2. Application Server: application server offers service to the user on call basis. The user can use any kind of service similarly PAAS(platforms as service), IAAS(Infrastructure as a Service) or SAAS(Software as a Service). It's the place where entire information of PHR owner is stored.
3. PHR Users: A PHR user is the one who is accessing the PHR data it may doctor, patient himself, family relatives, pharmacist etc. PHR users access the owner data only if owner authorizes them.

2.4Applications of PHR

Now a day's maintaining PHR is must since user can track their medical conditions Even while moving around. Cloud computing makes it easier for users to track their health conditions. Now a day's PHRs are emerging day per day. It can be used to check your current diagnosis, your medical history, medicines that you are consuming right now, doctor you are visiting etc. As self-monitoring technologies, have become more accessible and affordable, healthcare technologists have started to use tools like the personal health records (PHRs) to help patients become more connected with their health data. PHRs are technology applications that create a private and secure environment for users to access, manage and share their medical data. PHRs are essential for allowing patients to control their healthcare information and for acting as an engagement tool with their health practitioners. The primary consumers of PHRs are patients. The primary purpose of a PHR is to enable patient involvement in their care by handling their health information and to improve communication between the patient and their providers.

Some Applications of PHRs are as follows:

1. PHRs deliver users (patients) with in-depth information of their personal health situations and ability to track their progress. These further results in patients taking attention to progress their own health situations.
2. Mutual Communication among patients and physicians is easier and more operative with PHRs. This communication also benefits patients to share their medical accounts effectively with multiple physicians.
3. Patient engagement in the care procedure through PHRs gives them anchance to be part of their health choices as well.

2.5Advantages of PHRs:

Studydisplays that doctors who are in thepractice electronic health records have a tendency to better follow accepted treatment procedures and have a lesseramount of medication error. And one day, being able to view the data in your electronic health records on a computer, tablet, or mobile device is likely to help you stay wellup-to-date about your individual health. Right now, you may not be able to swiftly access your complete digital medical record. But progressively, healthcare providers are contributing a way for you to see some, but not all, of it once you enter a password—in what's called a patient portal. By logging on to a patient PHR, you can see the consequences of recent lab tests, for example, or can find out when you last had a tetanus shot. Some are set up so that you can email back and forth with your healthcare benefactor. With thehelp of PHRs you have the ability to share health information electronically so that you can be provided with the better care. PHRs help in providing better management care for the patients and also provide better care by:

1. It helps in providing the exact and up to date information about the patients.
2. It also provides easy access to the patient records for more efficient care.
3. It shares information securely and safely to other clinicians.
4. It also reducers medical errors and effectively diagnose of patients.
5. Improves the communication between the patient and health care centers.

6. It also enables safer and much more reliable prescription.
7. Also enables privacy and security to patient data.
8. Bring work-balance to life and improve productivity.
9. Helps in cost reduction by eradicating paper work and reduce duplication of tests.

2.6Literature survey on secure PHRs:

For the last few years security in PHRs has been an active research field, as cloud based PHRs are in its initial stage limited survey are available in various domains of PHRs. Here a survey on various researches did available in the field of PHRs. This report explores the various methodologies available in the field of PHRs.

1. Block chain challenges and security schemes a survey:

   In this paper Sonia Ben Rajibet al. describes about the current infrastructure that is being implanted which generally contains a centralized servers and relies on high speed broad band connection to provide data storage and computing services. He then described blockchain as new decentralized technology and then presented the advantages, disadvantages, limitations and area of application. This paper have also presented comparison of various block chain systems and their mechanisms.
2. Virtual Machine Migration Techniques:

   In this paper BhagyaLaxmiet al. proposed a mechanism of virtualization. In this technology multiple virtual machines are running on a single cloud server through which exponential increase in the number of cloud users is obtained. Through this demand of resources gets increased and them different resource management techniques are analyzed by moving single or multiple data centers. Papers also proposed comparison on various migration techniques available. At the end of the papers various issues that occur in VM migration technique are stated.
3. ComeHere: Exploiting Ethereum

   In this paper Matteo Franceshiet al. proposed a system that will be able to store medical records by using the blockchain technology. Through the blockchain

technology the user will be able to control and track the access rights. In this paper small implementation is performed which guarantees use of blockchain in PHRs and also discuss the future improvements as well as some issues that are still not resolved.

4. Efficient Fine-Grained Access Control for PHRs :

   In this paper kai heiet al. presented a new type of access control known as fine-grained access control. In this a new kind of proxy re-encryption server is used which is based on the identity of the user. The private key and cipher text size are kept constant and it is also proved that computational size does not depend upon the size of the message.

5. Requirements of Secure Storage Systems for Healthcare Records:

   In this paper RagibHasinet al. discussed the main characteristics about the health record management and presented a set of requirements so that we can achieve secure, reliable storage that follows the established regulations. They also analyzed the existing models and found out why these models are not suitable for use.

6. Secure and Privacy-Preserving Querying PHRs:

   In this paper Samira Baroutiet al. proposed a protocol through which health organization could produce statistical information by using encrypted PHRs that are being stored in the cloud. The protocol presented is dependent on two Homomorphic cryptosystems namely: Goldwasser-Micali (GM) and Paillier. Cryptosystems are used to construct KD trees from encrypted health records. The performance of the system is measured as the capability to process the SQL queries. The queries are executed on the encrypted data through the use of probabilistic cryptosystem.

7. Survey Paper presented on a Secure and Authorized De-duplication Systemby means of Hybrid Cloud Approach

   In this paper KirtiAshokraoTayadeet al. presented De-duplication technique in this technique all the repeated data in a particular data set is deleted. Problem lies in the fact that now data is first encrypted before it is sent to the user so it is hard to delete multiple copies if they exist thus data de-duplication technique comes

handy. In this multiple copies of data will be deleted and user will be left with one copy of data.

Athorough description of various sanctioned data de-duplication is projected to protect data security by with differential privileges of users in the identical verification. It introduced some new de-duplication designs that support an authorized duplicate check in hybrid cloudarchitecture, which creates the duplicate-check tokens of files from the private cloud server with private keys

.

CHAPTER 3
TECHNIQUES FOR SECURE ACCESS OF PHRs

Security of the data and the privacy of consumer data are the key challenges are framing architecture for cloud based PHRs. The data presented on cloud is always at risk since most of the implemented systems have loop holes in their security because of which data is always at risk of being corrupted. The security of data is measured in the terms of integrity of data, the access control and the type of encryption that is used. It is need to examine each category of work so that we can find out flaws that exist in the current system.

One of the key aspects to achieve secure sharing of PHRs is achieved by cryptography. So the main focus is always kept on the different ways of cryptography. Therefore, first we need to analyze different cryptographic techniques and then we will see the applications of cryptography in existing systems.

Apart from the security of data which we will be achieved through cryptographic systems it is also important to calculate the operational overhead. This should always be ensured that data as well as storage security must be provided with minimal amount of storage and computational work. The security of the data must always ensure authentication, authorization, confidentiality and integrity.

A lot of work has already been done on the security issues which are discussed below.

Nareshvurukondawith his team in his studies have shown the issues that we faces while storing data on the cloud data servers in which he have made special focus on issues regarding the identity management and access control. And after that he

had made some possible solutions that could help in eradicating some of the issues.

Ayesha Malik with her teamhave found out a procedure through which the users data and information could be protected in their studies they have clarified different features of cloud computing and have also discussed diverse service models.

Yunchuan Sun with his team have performed a review on the different security solution available and also reviewed the different privacy protections in cloud computing. As a conclusion they have presented an empirical research analysis on different approaches to the security.

Mazhar Ali with his team havepresented different issues of security involved in the cloud computing. In their survey they have presented the modern security solutions along with the complete discussion of the security issues. Sultan Aldossaryand team members have shown the problems that we faced in the cloud data storage and solution that are available. In their studies they have shown the issues related to the virtualization as well as the data integrity, availability, confidentiality.

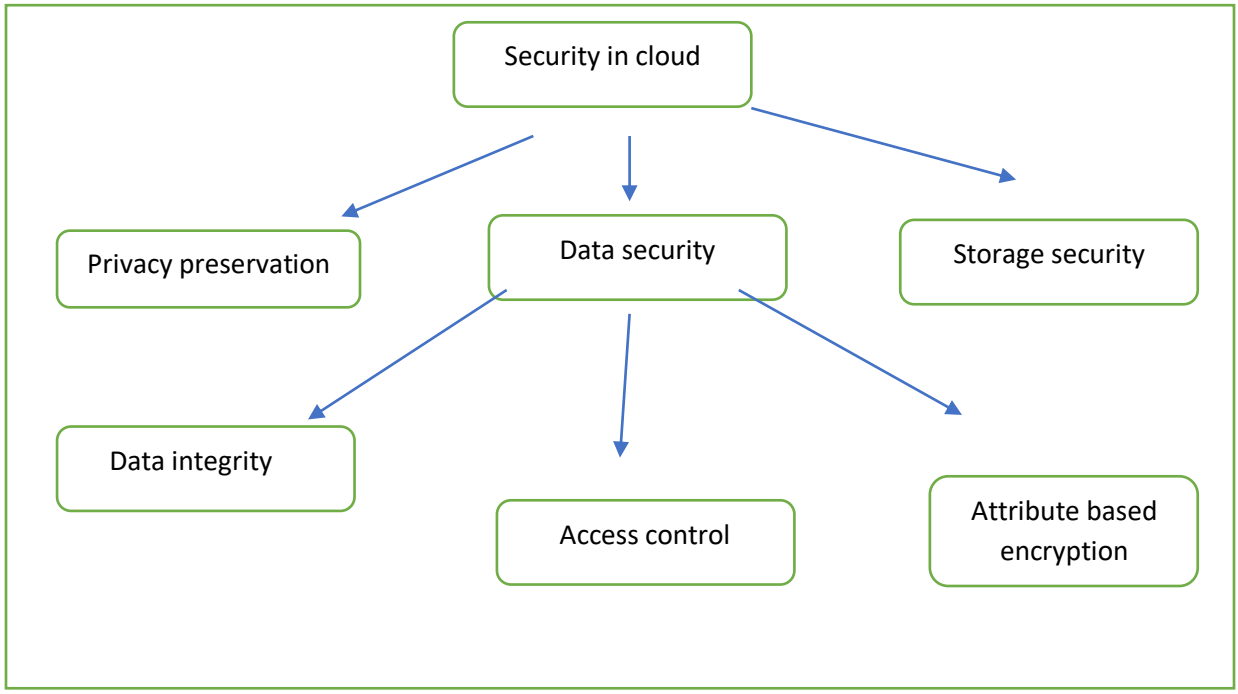

Fig 3.1 Classification of security

3.1 Current work going in Privacy protection

HaralambosMouratidisand team members offered security framework tochoose a cloud provider on the base of certain definite requirements. In this we will use aModeling language and some tools such as Open Model Initiative (OMI) platform. The language is used to apply the fundamentals of the security and privacy.

L. Malinaand team membersprojecteda prototype in which security is implemented based on group signatures. In this model security is based on the anonymity of the user. This is also ensuring the confidentiality as well as integrity of the communicated data.

Ulrich and team membersplanned a model in which design is provided in such a way that it prevents the illegalcontact of uploaded informationfrom the internal and external data managers. It's using XACML structure for explanation and access control policy. Finally, the contents are encrypted by means of an encryption policy.

3.2 Current works on Storage Security

Kan Yang and team members presentedan auditing procedure for cloud system to preserve privacy. The protocol is used to support dynamic operation on information and batch auditing in order to support the multi cloud environments. Bilinear pairings is used to produce an encrypted proof. Data auditor confirms the proof of correctness. Entire computational overhead is now moved to the cloud server from the auditor. Only disadvantage is that it can't provide confidentiality and integrity to the user.

Qian Wang and team members provided a scheme in which confirmation is done by mixing data integrity and dynamic informationactions. An examiner is used to demonstrate the integrity of the storage data. Block insertion and Merkel Hash Tree is used to provide the data operations. Multiple auditing tasks have been maintained through the application of bilinear aggregate signature.It is not enough to provide the confidentiality and the authorization.

Yan Zhu and team membersplanned a Provable DataPossessions (PDP) toguarantee integrityof the cloud data storage. In PDP, many cloud service providers cooperatively effort to preserve the data of the client. Homomorphic provable responses and hash index

are two main apparatuses to preserve hierarchy. It also gives guard against leakage of the data and counterfeit of the tag attacks. Major drawback is that it does not deliver confidentiality and the authorization.

3.3 Current work in the field of data integrity

Laicheng Cao and team membersgave aMobile Multi Clouds Data Integrity Verification scheme (MMCDIV). In this systemlive data actions and integrity confirmation is completed by light weight computational methods. It will not offer the confidentiality and authorization. It's also rests onone TTP server thus may get crashed at some times.

Nedhal A. Al-Saiydand team membersplanned cloud computing security model he also conferred the cloud security risks. It also defined various methods to offerresolution to security fears cloud computing. It flops to provide any typical algorithm or method to provide the data integrity.

3.4 Current works on Access Control

Younis A. Younisand team membersplanned an Access Control model aimed at the Cloud Computing (AC3)to satisfy the condition of the access control. It preserves three hierarchal which are founded on the level of trust.Given model categorizes the users according to their roles which control their security fields. This does not bring confidentiality and integrity.

Jin Li and team membersplanned a finegrained access system which is created on ABE. In this access control rules are defined based on the characteristics of the data. Traitor tracing method is used to analyze the accountability of the user. This technique results in large amount of messages overhead.

Yan Zhu and team membersoffered an encryption scheme aimed at temporal access control (TACE). Algorithm practices access policy in which the temporal attributes describes the access rights of the handlers. TACE employs temporal constraints. This technique does not guarantee confidentiality and integrity.

3.5 Current works on ABE

Saravana Kumar and team membersprojectedinnovative encryption technique which is built on ABE. In this technique we used digital signature as well as asymmetric encryption algorithm along with the functions. But meanwhile the encryption is created on simple hash encryption data can be corrupted.

Shulan Wang and team membersprojected file hierarchy that is built on ABE scheme for the cloud computing.This arrangementuses integrated access control to encrypt the hierarchical files.The files share the cipher text shares of the attributes. This scheme does not offer the data integrity. It's also reliant on a single Third-party auditor which can be crashed at any time.

Shulan Wang and team membersprojectedabetter two-party key delivery protocol. This procedure is intended in such a way that the key can't be conceded either by key manager or Cloud service provider. They have also allocated weight to individualcharacteristicto recover the expressions of the attribute. This thing drastically reduced the storage cost and encryption cost.

Table 3.1 Comparison of Existing Schemes

Authors	Method	Service	Privacy	Confidentiality	Integrity	Access Control	Storage Security
Younis A Younis and team members	Cloud computing using Access Control Architecture	Secure access permission for multiple services	No	No	No	Yes	No
Varsha D Mali and team members	User Authentication and Access Control Technique in Cloud Computing	Cryptographic RBAC	Yes	Yes	No	Yes	No
Jin Li and team members	Fine-grained Data Access Control Systems with User Accountability	ABE	No	Yes	No	Yes	No
Guoyuan Lin and team members	Trust Based AC Policy	Trust Management, role-based access control	No	No	No	Yes	No

Yan Zhu et Al	Temporal Access Control	Temporal access control Encryption, proxy-based re-encryption	No	Yes	No	Yes	No
Saravana Kumar and team members	Enhanced ABE	ABE using digital signature and asymmetric encryption	No	Yes	Yes	Yes	No
Shuln Wang and team members	An Efficient File Hierarchy ABE Scheme	ABE using Integrated access structure	No	Yes	No	Yes	No
Shulan Wang and team members	Attribute-Based Data Sharing Scheme	Two-party key issuing protocol, weighted	No	Yes	No	Yes	No
Tran Viet Xuan Phuong and team members	Hidden Ciphertext Policy	ABE using hidden access policy	No	Yes	No	Yes	No
Entao Luo et al	Hierarchical Multi-Authority and ABE Friend Discovery Scheme	ABE using multi authority, friend discovery schemes	No	Yes	No	Yes	No

Nedhal A. et al	Data Integrity In Cloud Computing Security	Data Integrity checking algorithm	No	No	Yes	No	No
Laicheng Cao and team members	Data Integrity Verification Scheme	Mobile Multiple cloud Data integrity Verification	No	Yes	Yes	No	No
Ali Mohammed Hameed Al-Saffar and team members	Identity Based technique	Data integrity and Confidentiality in the multiple cloud environment.	No	Yes	Yes	No	No
Edoardo Gaetani and team members	Block chain-based Database to Ensure Data Integrity	Integrity verification using Block chain database	No	No	Yes	No	No
L. Malina et al	Privacy-preserving security solution	Non bilinear group signature scheme	Yes	Yes	Yes	No	No
Haralambos Mouratidisa and team members	A framework to support selection of cloud providers	Modelling language and selection of CSP	Yes	No	No	No	No

Ulrich GrEveler et al	Cloud Computing with a System that Preserves Privacy	Trust model prevents CSP from accessing outsourced data	Yes	No	Yes	Yes	No
Lifei Wei et al	Security and privacy for storage and computation	Discouragement of Privacy cheating and auditing of secure computation	Yes	No	Yes	No	Yes
Yan Zhu et al	Cooperative Provable Data Possession for Integrity Verification	Homomorphic verifiable response and hash index hierarchy	No	No	Yes	No	Yes

3.6 TECHNIQUES USED IN EXISTING SCHEMES

3.6.1 Diffie-Hellman Key-Exchange

We use Diffie-Hellman Key Exchange so that we could achieve secure distribution of keys among two persons.This algorithm resolves the problem of key being stolen by an intruder. To understand this thing let's assumeAntony and Bhuvineeds to share key but the channel they are using for the transmission process is not reliable. Their info can be seen by some third person Tony. The solution to this problem is to share the key amongAntony and Bhuvi without making it presented to Tony. This thing could be achieved by using Diffie-Hellman key exchange. It contains following steps:

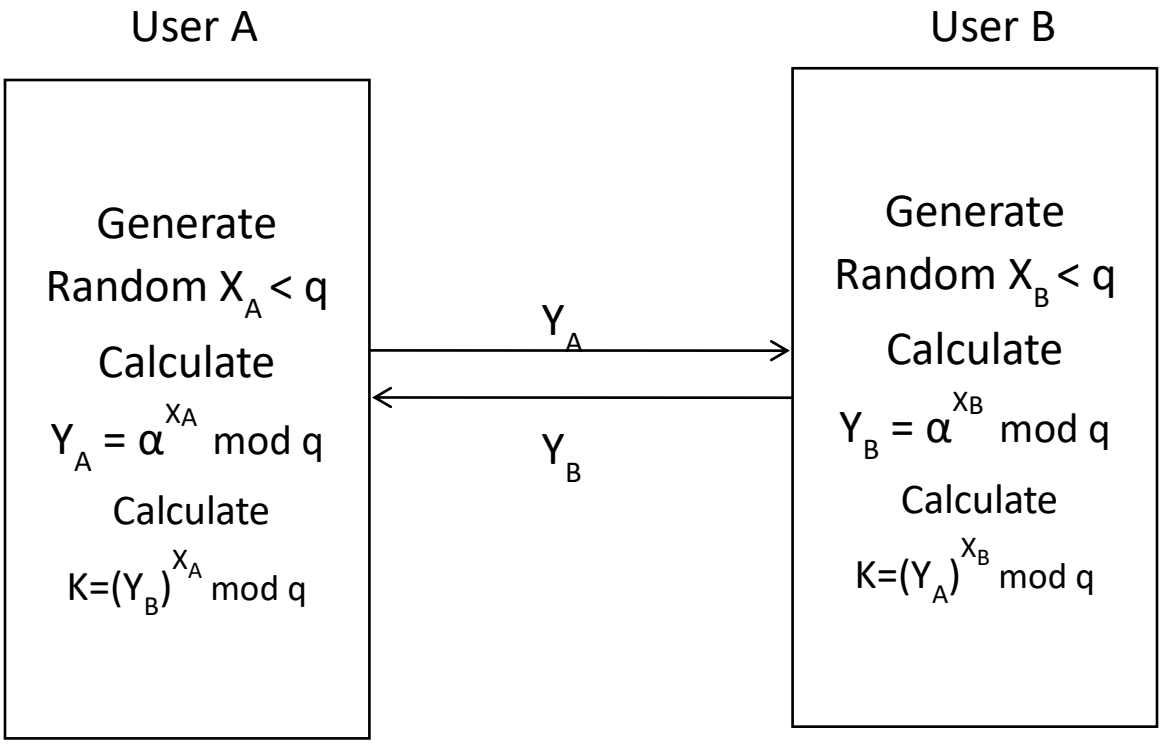

Fig 3.2 Diffie Hellman Key Exchange

3.6.2 Bilinear Pairings

We will now assumeK1, K2 to be apart of agroup of order p. K1 will belongtoanadditive group whereas K2 willbelongto a multiplicative group.

K1 = <P>

Bilinear Mapping on (K1 ,K2) is :

e: K1 × K1 → K2

Thatfulfills the following conditions:

1. Bilinearity: For allV,E∈K1 and a, b ∈ ZV *, e(aV;bE) = e(V;E) for all V,E∈K1 and all a, b ∈ Z.

2. Non-degeneracy: This map will not send all pairs in K1 × K1 for the identity in K2. e(V,V) is a generator in K2 .

3. Computable:The algorithm provided is efficient one to compute e (V;E)for any V,E∈K1

Any map that satisfies these three criteria's is said to be a admissible bilinear map.

3.6.3 Merkle Hash Tree (MHT)

The name of this tree comes after a great scientist named Ralph Merkle. This tree can be constructed in the form of a binary treewhere leaf nodes are actually the hashed value of authenticated data value. It is good in providing the confirmation to the data and also verifies that the data is unchanged unharmed and is secured. This tree is itself a data structure that contains summary of a larger piece of data.

The examples of the hash functions that are used for hashing are Whirpool and SHA-1. This tree is being used to check whether it was possible to send data in correct manner or not.

3.6.4 Proxy re-Encryption

In these techniques we will allow third-party to change a cipher text which already has been encrypted for someone so that it can be decrypted by another one. To explain how it works take an example:Bhuvi will designate a proxy re encode one of his messages that are being sent to the Chris. This thing will generate a new key that Chris will use to decode message. Now suppose Antony wants to send Chris a message that was being encrypted by Bhuvi's key the proxy will then change the messagesin such a way that Chris can be able todecrypt the messages.

3.6.5 Identity based Encryption

This form of the encryption uses an arbitrary string which will serve as the key. While during the time of decryption, a decryption key is being mapped to a random encryption key which is done by the key management authority. This kind of encryption comes under the category of public key encryption in which the public key of the user is some kind of unique information which is related to the identity of that specific user. The motivation for this scheme comes through the need for the deployment of the public key infrastructure.

3.6.6 Symmetric Encryption Algorithm

In this technique of cryptography, we encrypt or decrypt the data. There are many names to this technique such as encoding and decoding, enciphering and deciphering. In this we use the process of encryption to change the plain text into some unknown string of text called cipher text. With the help of encryption, we can hide the real meaning of our text. Another process is decryption on which we will take some cipher text and then convert it into the plain text.

If we will use the same key for the process of encryption and decryption then its known as symmetric encryption. Eg: DES, AES and Bowlfish.

3.6.7 Incremental Cryptography

Increment cryptography focus on developing those cryptographic algorithms in which if we wish to add more text to our cipher then we don't need to convert the entire text again. To understand this suppose we have a text file A which we have ciphered now we wish to add some more information to the A in this case we want our algo to be in such a way that we can simply append the information to the A without any extra effort.

3.6.8 El Gamal Encryption

El Gamal Encryption comes under the category of public key cryptographic algorithm which is an kind of asymmetric keys encryption algorithm. This algorithm is built on Diffie-Hellman key exchange algorithm. This algorithm was first presented by Taher El Gamal in year 1985.

This algorithm relies on difficulty indiscrete logarithms of a cyclic group which means even if we get know $X^A$and X^K its very hard to compute the value of X^{AK}.

The El Gamal encryption is divided into three main portions:

1. Key Generation
2. Encryption of data
3. Decryption of data

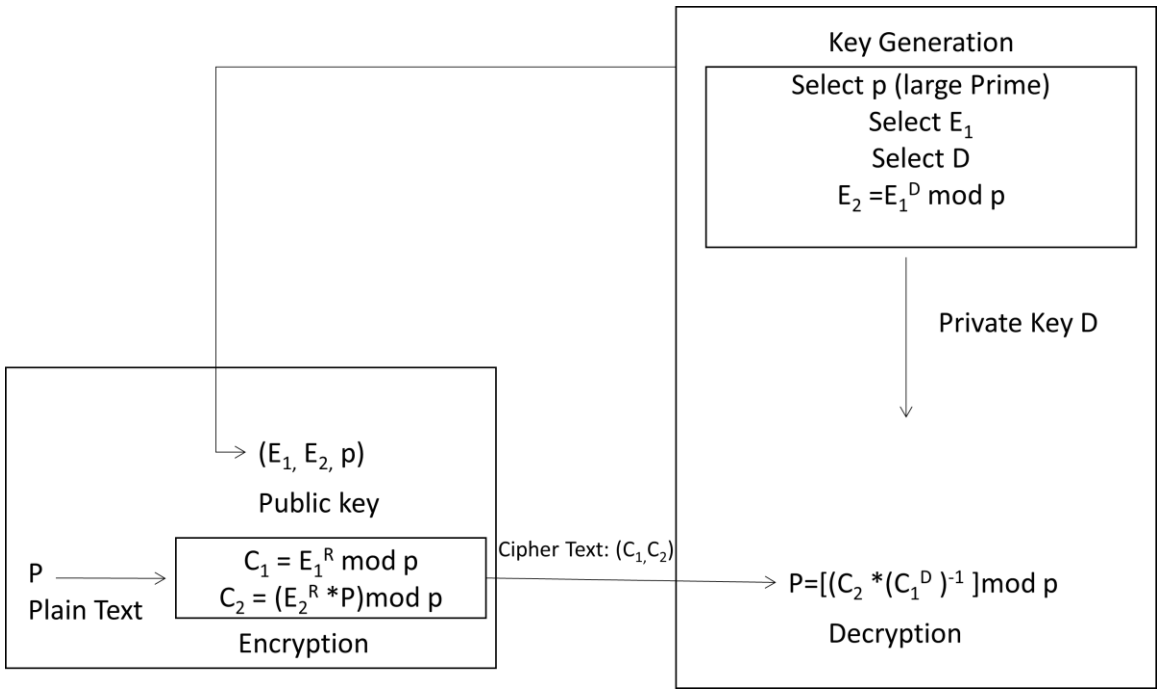

Fig 3.3 El Gamal Encryption

Chapter 4

Proposed Solution

In this segment we will discourse about the mechanism that we adopted to ensure the secure sharing of ePHR in cloud computing architecture.

While designing a perfect secure PHR we should first ensure that the entire PHR data should only be authorized by the owner itself only PHR owner could decide to whom you can show the data and how much data should be visible to an individual. Secondly entire data should be stored on cloud server in encrypted form only so that Even if someone is able to breach the server he would not decrypt the data.

The data server and the server where keys are stored should be separated to bring security to the data.

Thus In our approach we have guaranteed that the full control of the PHR will be in the hand of the owner and this is how it ensures the privacy of the PHR. Owner can grant different level of access to different PHR data users. A partial trusted proxy server is also being setup that will produce public/private key pairs as well as re encryption keys.

The vitalfundamentals of the projectedproject are mentionedbelow:

• We will provide a procedure that will permit patient to control the distribution of their individual PHRs at the cloud.

• Thisprocedureusesfamous El-Gamal encryption by Tamur El-Gamalalong-with proxy re-encryption so as to approve thePHR secrecy.

• Thisstrategywill allow the PHR possessorswith the power to selectively allowparts of the PHR which will be visible to other users. This thing will depend on the access levelstated in the ACL for different groups of handlers.

• A partially trusted proxy server named as Re-encryption server will be brought in the scheme that will promise the access control and it will also be responsible to produce the

asymmetric keys to the users. It will assign keys to the newly registered users and will delete the keys of the old users.

• Along with this we will providebackward and forward access control is also implemented in the projectedtechnique.

Suppose if there is a user that want to access a little portion of PHR, firstly the individual will download PHR from the cloud only afterward the authentication. The downloaded PHR will be in the encrypted form only so even still at this point the user will not be able to decrypt the PHR thus user will ask SRS to provide appropriate decryption parameters. Then SRS will check the Access Control List and then it will determine if the access to the part for which user has wished the decryption parameters arearranged by PHR owner or not. And then in accordance to the Access permissions specified the SRS will send the corresponding parameters to the requesting user.

4.1 Architecture of the proposed solution

The architecture that we are using includes a PHR owner, Cloud Data Server, Re-encryption Server, PHR users. The proposed architecture is shown in the fig 4.1

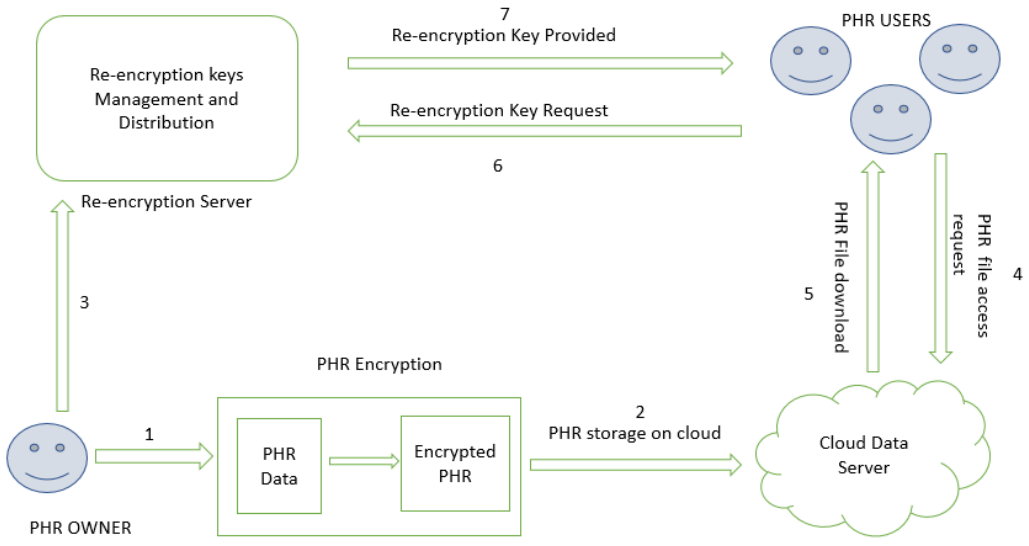

Fig 4.1 Architecture of proposed solution

1. PHR Owner: PHR Owner is the one who owns that particular PHR. In our method we have tried to partition data of the PHR into different sectors such that each part could be encrypted/decrypted separately.
2. Cloud Data Server: Data Server is the place where the entire PHR figures are being kept. On the cloud server the information is kept in the encrypted form so that no un-authorized person could see the data.
3. Re-encryption Server: Re-encryption server performs the task of generating the keys and then distributing the keys among different PHR users depending upon their access levels. Every time a new user gets connected Re-encryption server will place a public/private key pair for that user.

   When an old user will be removed his keys will automatically gets deactivated and get removed from the server.
4. PHR users: they are the ones who wishes to access the PHR data they will first asks for encrypted PHR from cloud data server then request owner to grant them access to decrypt

   The file owner will then transfer approval to Re-encryption server to grant him parameters to decrypt the file.

Participant	Role
PHR owner	PHR owner is the one who uses the cloud server to upload the PHR information.
Cloud Data Server	Provides the storage for the users to upload the PHR data.
Re-encryption Server	Provides and manages the encryption/decryption keys.
PHR user	Anyone authorized who wishes to use the PHR of an individual.

Table 4.1 Role of Participants

4.2 Working of Proposed solution:

In this section we will explain the working of our solution and will tell how the flow of data will take place in the proposed architecture. We will explain step by step how our data is being uploaded to the cloud data server and how the encryption and decryption parameters are being uploaded and used. In our architecture we have maintained two servers first one is cloud server that will be responsible for data upload and download in our case data is the PHR of the patient and another one is Re-encryption server which will be responsible for the key management, user registration and deletion, access control.

Cloud Data server is the one where all the information is stored in encrypted form and Re-encryption Server is responsible for the public/private key generation, key distribution and management also it will check the access levels for different users.

First of all as soon as we will register a new user the user registration request will first go to the Re-encryption server in our case Re-encryption server may be seen as the administrator, after this re-encryption server will decide whether or not to activate that user. Re-encryption server will accept the registration request of only the authenticated user if some how it feels that user is not authenticated the server will decline the registration request; as soon as Re-encryption server will activate the user it will store the public private key pair for that user. For generating the public private keys pair we are using an asymmetric encryption algorithm that is El-Gamal encryption algorithm in our approach we are assuming our channel to be secured. After this step the keys will be transferred to the user so that he can encrypt the data. After this the entire information of the PHR user will be encrypted by using the keys generated by the re-encryption server and gets stored in the cloud data server. The encrypted PHR data could be accessed by anyone using the system only after the approval of the PHR owner. When someone wishes to access the PHR he will first send a request to the owner of the PHR to send him parameters to decrypt the file after this he will download the encrypted PHR from the cloud server. The PHR owner will send his approval to the Re-encryption server then re-encryption server will check the access list and decide how much part of data should be visible to that user and accordingly will send him parameters. Upon receiving parameters the user could decrypt and read the file and could make some changes if he is allowed to

do so after that the updated file is again encrypted but now from different key sets this is done by re-encryption server, changing the keys is must since user has seen the keys and now its not safe to use the same keys again so re-encryption servers will generate a new pair of keys, and will be uploaded to the cloud data server.

Chapter 5

Analysis

We will analyze our planned scheme by investigating two kinds of studies:

1. Parameters related to security
2. Parameters related to performance

All the things that we examine Security study isprojected towards the scheme in which we will analyze or examine all the probable security threats. The main thing that we will focus upon here is that we will see if our mechanism is examined against its exactness and whether or not it will offer the security and confidentiality to the users.

When we talk about performance evaluation then the projected scheme is examined against all the actions that are involved in the scheme we will also discuss the storage necessity of the scheme.

5.1 Security Analysis:

We havenumeroussecurity providers thatgrants security to their cloud systems, the thing where they fail is that the encryption as well as decryption process is done on the server end. Along with this they also do not provide any kind of reliable data integrity mechanism.In ePHRs data is easily accessible on the cloud and any one can easily get the data.In our proposed scheme we are granting the integrity of the data and we will verify the integrity as well. We will be able to provide data in confidential manner so that only the authorize persons will be able to see the information because of which data will not be unveiled to any unauthenticated person. Since we have encrypted the data with the one of the most prevailing encryptionalgorithm it is almost impossible to decrypt it without the symmetric key.

There are following security examinationsachieved:

1. Correctness: In this Scheme first, an Authenticated individual could decrypt the file and even he can only decrypt the portion of the file for which he has been allowed by the owner of the PHR. So the correctness of scheme is guaranteed.
2. Privacy as well as Confidentiality: The file movedamong those of Users and Cloud Storage administrator is already encrypted and encoded, thus the cloud data provider could not read the data of the file and thus the authenticity and integrity of the data is maintained. Here before transferring the file to the cloud user encrypts the file so while file is being transferred to the cloud through any channel it's not common text so any intruder who wishes to read the file will fail to do so.
3. Hacker Attack: In internet, a hacker can attackdataanytime from anywhere. In this scheme we are using the internet to transmit our messages so there is always a risk that message could be condemned in transmit by the hacker. In this scheme even if hacker attack the messages in transmit he will not be able to decode the message since he need the keys to decipher the message. And the encryption algo that we used is strong enough that it can't be break.

5.2 Studying the performance parameters

The performance of the following mechanism is measured in two parts the first one is the amount of space that it will consume and the other one is the time it will take to encrypt and decrypt the message.

Here the data cloud server has enough amount of storage for loading the user PHRs so there is no need to ponder upon the storage requirement. The Re-encryption server requires only storing the keys that are of constant size thus it is not a very big deal. Here only the encrypted file is kept on at the cloud storage thus the goals required for storage are already fulfilled.

Regarding time complexities we are using el- gamal encryption for our cipher text process this algorithm takes a little extra time compare to RSA algorithm while generating the keys but the advantage over RSA is that it decrypts faster than RSA.

CHAPTER 6

Experimental Results

In order to simulate the concept of the architecture designed in chapter 4 we have designed and implement a web based application. The application will run on the local host server. We are assuming that PHR data owner, Re-encryption server, cloud data server all reside on the same network and share the same system parameters. Whenever a user wants to upload his PHR to the cloud data server he will first encrypt the data and then upload it to the cloud server. Thus in this case the encrypted file gets stored on the cloud server so that on unauthorized person could see the file.Figure 6.1 shows the user registration field builds for the owner of the PHR.

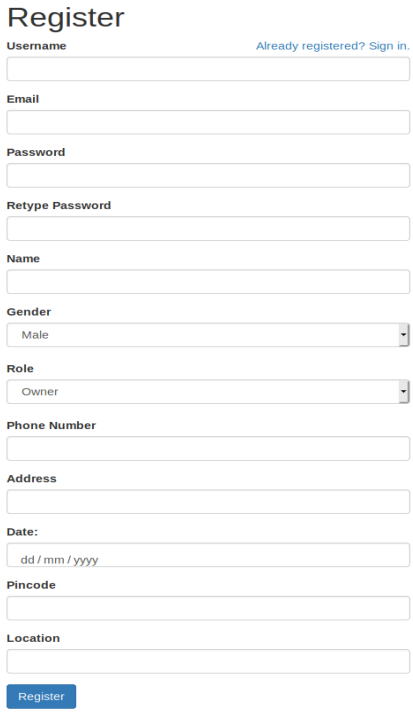

Fig 6.1 user registration forum

Through this form the user will be able to register his information on the cloud data server. The user will first of all have to enter every detail mentioned in the form and then when he will push submit button his request for the registration will go the Re-encryption server as shown in the figure 6.2.

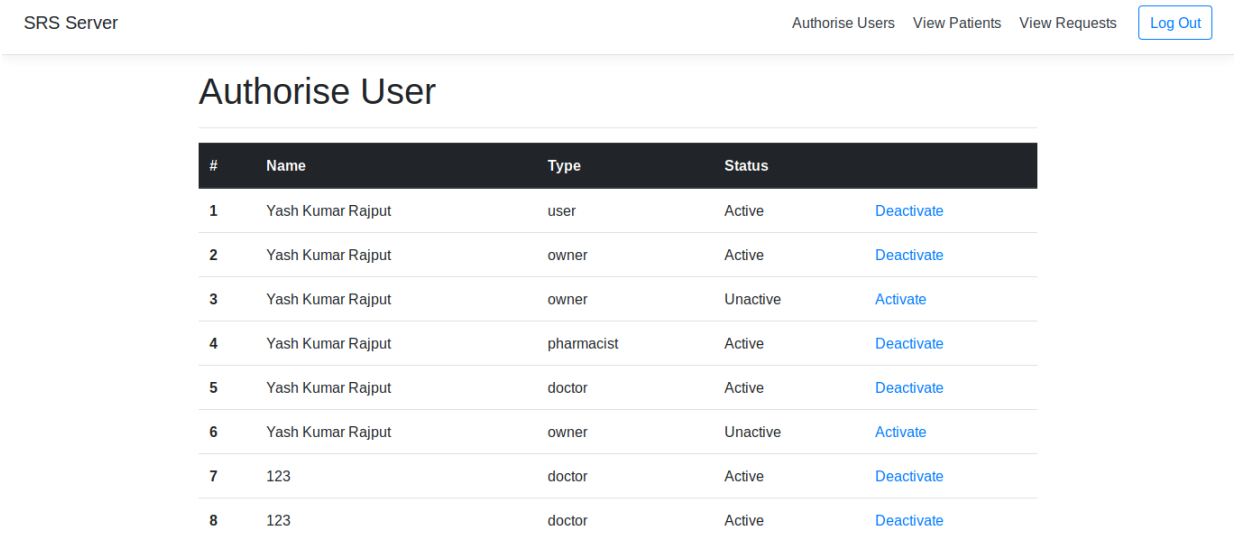

Fig 6.2 SRS manager interface

SRS server will decide whether to activate or deactivate the user. Upon activating the user the data will be uploaded to the cloud data serverin the encoded form as shown in the fig 6.3.

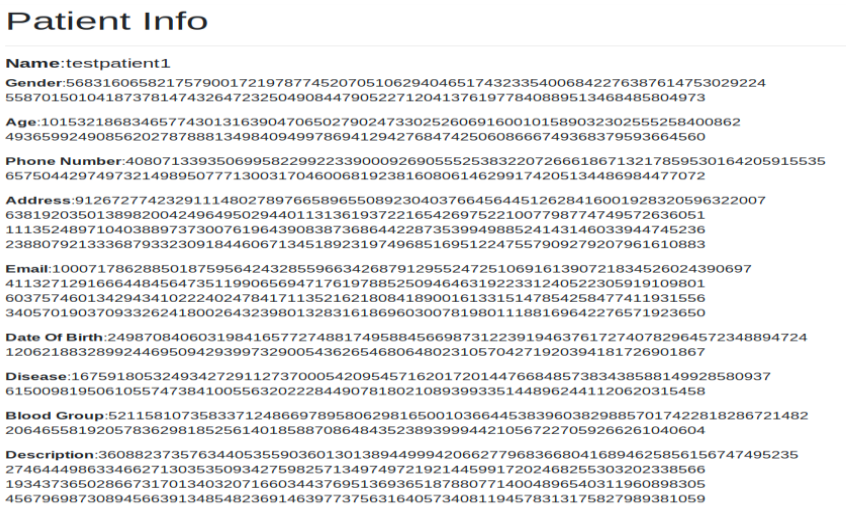

Fig 6.3 PHR encrypted form

Now when a user will need to access the PHR of a user he will ask for the decryption parameters from the proxy re encryption server depending upon the access control the re encryption server will grant parameters to the user for the decryption process.

Chapter 7

Conclusion and Future Work

We projected a methodfor safely storing and spreading of the PHRs to the authorized users. The methodguards the secrecy of the PHRs also authorizes a patient-driven access control to different parts of the PHRs reliant on level of the access provided by the patients. We characterized a fine-grained access control policy so that even the central framework clients will not be able to get to those bits of the PHR for which they are not permitted. The PHR proprietors store the encoded data on the cloud and just the appropriate users having significant re-encryption keys issued by a semi- trusted intermediary can decode the PHRs. The job of the semi-trusted intermediate proxy server is to produce and store the bar public/private key sets for the clients in the framework. In addition to saving the classification and guaranteeing patient-driven access power over the PHRs, the methodology likewise directs the forward and in reverse access control for leaving and the recently joining clients, respectively.

Future works include studying the more advanced encryption techniques such as implementations of Attribute based Encryption and making the network channel much more secure. The proxy server we are using is semi trusted we can increase the security of these servers in our future works.

Chapter 8

References

1. Abbas, K. Bilal, L. Zhang, and S. U. Khan, “A cloud based health insurance plan recommendation system: A user centered approach, 2015.

2. A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, “Incremental proxy re-encryption scheme for mobile cloud computing environment,” 2014.

3. L. Ibraimi, M. Asim, and M. Petkovic, Secure management of personal health records by applying attribute-based encryption,Technical Report, University of Twente, 2009.

4. Amini Abbas, “Secure Storage in Cloud Computing. Technical University of Denmark, DTU Informatics” 2012.

5. Gehani, Ashish La Bean, Thomas H. Reif, H.John, “DNA – Based Cryptography”, Dimacs Series in Discrete Mathematics and Theoretical Computer Science, 54:233-249, 2000.

6. SouhilaSadeg “An Encryption algorithm inspired from DNA”, IEEE pp 344 – 349, November 2010

7. K. Gai, M. Qiu, “Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers,” 2017.

8. M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, “A general framework for secure sharing of personal health records in cloud system,” 2017.

9. L. D. Moura and N. Bjørner. "Satisfiability modulo theories: An appetizer." In Formal Methods: Foundations and Applications, Springer Berlin Heidelberg, 2009.

10. A. N. Khan, M.L. M. Kiah, S. U. Khan, Sajjad A. Madani, and Atta R. Khan. "A study of incremental cryptography for security schemes in mobile cloud computing environments" 2013.

11. F. Xhafa, Fatos, J. Feng, Y. Zhang, X. Chen, and J. Li, “Privacy aware attribute-based PHR sharing with user accountability in cloud computing,” 2014.

12. K. Gai, M. Qiu, and X. Sun, “A survey on FinTech,” Journal of Network and Computer Applications, 2017.

13. A Anusha, Kranthi Kiran G and J Dayanika , “Compressing the Data Secure Authorized Deduplication Checker in Hybrid Cloud” 2015.

14. Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P.C. Lee, and Wenjing Lou, “A Hybrid Cloud Approach for Secure Authorized Deduplication” 2015.

15. P. Ashok kumar, S. Saradha, “An Efficient Security Based Authentication for Cloud Storage”, 2016.

16. Ekblaw, A., Azaria, A., Halamka, J.D., Lippman, “A case study for blockchain in healthcare: medrec prototype for electronic health records and medical research data” 2016.

17. H. Nie, P. Li, H. Xu, L. Dong, and J. Song, “Research on Optimized Pre-copy Algorithm of Live Container Migration in Cloud Environment” 2017.

18. H. Li, G. Zhu, C. Cui, H. Tang, Y. Dou, and C. He, “Energy-efficient migration and consolidation algorithm of virtual machines in data centers for cloud computing,”2016.

19. K. C. Nguyen, V. S. G. Dong, N. H. Son, and H. D. Loc, “An Efficient Virtual Machine Migration Algorithm based on Minimization of Migration in Cloud Computing,” 2016.