Savitribai Phule Pune University.

A DISSERTATION REPORT ON

A Methodology for Secure Sharing of Personal Health Records in Cloud Environment.

SUBMITTED TO THE UNIVERSITY OF PUNE,PUNE
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE AWARD OF THE DEGREE

MASTER OF ENGINEERING

(Computer Engineering)

Second Year

BY

Shaikh Aaliya **Exam Seat No:12789**

Under the Guidance of
Dr Bendre M.R.

DEPARTMENT OF COMPUTER ENGINEERING
Vishwabharati Academy's College Of Engineering,
Sarola Baddi, Ahmednagar 414201
2018-2019

DEPARTMENT OF COMPUTER ENGINEERING
Vishwabharati Acadmey's College Of Engineering
Sarola Baddi, Ahmednagar 414201

C E R T I F I C A T E

This is to certify that the Dissertation Report entitled

" A Methodology for Secure Sharing of Personal Health Records in Cloud Environment"

Submitted by

Shaikh Aaliya **Exam Seat No:12789**

is a bonafide work carried out under the supervision of Prof. and it is submitted towards the partial fulfillment of the requirement of Savitribai Phule Pune University, Pune for the award of the degree of Master of Engineering(Computer Engineering).

Prof.	Prof.Bendre M. R.
(Internal Guide)	(M.E.Coordinator)
Prof.Aher S. M.	Dr. Makasare P. A.
(HOD Computer Dept.)	(Principal,VACOE,A'nagar)
Internal Examiner	External Examiner
Place: Ahmednagar	Date:

CERTIFICATE BY GUIDE

This is to certify that Shaikh Aaliya has completed the Dissertation Stage I work under my guidance and supervision and that, I have verified the work for its originality in documentation, problem statement,and results presented in the seminar. Any reproduction of other necessary work is with the prior permission and has given due ownership and included in the references.

Place: Signature of Guide

Date: (Dr.Bendre M.R.)

ACKNOWLEDGEMENT

A successful work of Dissertation is the result of inspiration, support, guidance, motivation and cooperation of facilities during study. It gives me great pleasure to acknowledge my deep sense of gratitude to present my seminar titled: "A Methodology for Secure Sharing of Personal Health Records in Cloud Environment".I would like to give sincere thanks to our Principal Dr.Makasare P.A. and H.O.D Prof.Aher.S.M. for giving me opportunity to present this seminar. I am also thankful to my respected guide Dr. Bendre M.R. I for their whole-hearted support and affectionate encouragement without which my successful seminar would not have been possible. Last but not least I have to express my feelings towards all staff members of Vishwabharati Academy's College of Engineering and special thanks to my friends for their moral support and help.

List Of Publication and Conferences

International Engineering Research Journal (IERJ), ISSN 2395-1621, Volume 3 Issue 1 Page 4902-4904, 2018.

Paper Title: A Methodology For Secure Sharing Of Personal Health Records In The Cloud.

The 6th Post Graduate Conference of Computer Engineering (cPGCON-2019) 3rd -4th April 2019.

Paper Title: The Privacy Based Secure Sharing Of Personal Health Records a Method in the Cloud

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162), JETIR1905E19 Volume 6 Issue 5 , May- 2019

Paper Title: The Privacy Based Secure Sharing Of Personal Health Records a Method in the Cloud

ABSTRACT

Now a day every information is stored and shared on the cloud. And so the medical record especially Personal Health Record (PHR) is an important part of health information exchange, that is need to be stored at cloud servers. But there are various privacy problems as personal health information could be discovered to unauthorized people. That need guarantee of the patient control over to their own PHRs, in this method encryption of the PHRs is done before the storage on cloud. But still issues like risks of privacy, efficiency in key administration, flexible access and efficient user administration, have still remained the important challenge toward achieving better, cryptography imposed data access control. In this research development, we develop a mechanism for control of data access to PHRs stored in cloud servers. To achieve this efficient and modular data access control for PHRs, we provide encryption approach for the encryption to each PHR file. For this system method already tried to focus on the multiple data ownership scheme also dividing the users into security domains that highly reduce the key management complication for owners and users. Here the system takes patient privacy as serious issue and guaranteed it by exploiting multi-authority Encryption. Our main aim is not only privacy but also systems scheme try to enable modification of access policies or file attributes, and break-glass access under emergency situations. Our proposed scheme shows Extensive analysis and experimental results are presented for security and efficiency of PHR.

Technical Key Words: Access control, Cloud computing, Medical Services, multi-authority Encryption, Privacy, PHR

SYNOPSIS

Dissertation Title

A Methodology for Privacy Based Secure Sharing of Personal Health Records in Cloud Environment.

RESEARCH AREA OF THE PROJECT

Cloud Computing

Technical Keyword

Cloud Computing

As cloud computing is the newest term for the long-dreamed vision of computing utilities. The cloud provides on-demand network access to a centralized pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Nowadays Cloud computing is rapidly changing the internet service enabling the small organization to build mobile application for users. Cloud computing is a significant advancement in the delivery of information technology and services. Cloud computing builds off a foundation of technologies such as grid computing, which includes clustering, server virtualization and dynamic provisioning, as well as SOA shared services and large-scale management automation. Cloud computing is referred to a model of network computing where program or application runs on a connected servers rather than on a local computing device. Cloud computing relies on sharing of resources to achieve coherence. By this cloud computing is the broader concept of converged infrastructure and shared services.

Multi authority encrytion

Cloud providers use the distributed model to enable lower latency and provide better performance for cloud services. Beyond the cloud provider context, two other examples of distributed cloud are public resource computing and the volunteer cloud. Public resource computing is a cross between cloud computing and distributed computing that involves computers in geographically dispersed locations connected to collaborate on compute-intensive and/or computer-intensive tasks. Some examples of this are Folding@home, BOINC and SETI@home. In a volunteer cloud, the resources of member computers are connected through a single service or hub to collaboratively construct and configure cloud infrastructure.

PHR

Use of cloud services has taken off across countless industries. Adoption of cloud computing in healthcare has taken place a little more tentatively, as providers sort out how they can benefit from cloud offerings and how much of their operations they can afford to transfer to the cloud. EHRs, analytics and imaging systems are a few areas in which healthcare providers have found success with

cloud deployments.The flexibility of cloud hosting is one of its upsides, while initial conversion costs and the security of the system and the data it hosts are two major concerns that have some organizations dubious of the sustainability of cloud computing in healthcare. Care providers aren't alone in looking for ways to implement cloud hosting services. Some cloud providers are adjusting their products to fit healthcare needs. Also, an established EHR titan made news by announcing the construction of a cloud data center. These developments are only part of the ongoing maturation of cloud in healthcare.

Privacy

Unauthorized users without appropriate privileges or files, including the cloud server, should be prevented from access to the underlying plain text store. In another word, the goal of the adversary is to retrieve and recover the files that do not belong to them. In our system, compared to the previous definition of data confidentiality based on convergent encryption, a higher level confidentiality is defined and achieved.

Access Control

In the fields of physical security and information security, access control (AC) is the selective restriction of access to a place or other resource.[1] The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.Locks and login credentials are two analogous mechanisms of access control.There are three types (factors) of authenticating information:

1. Something the user knows, e.g. a password, pass-phrase or PIN
2. Something the user has, such as smart card or a key fob
3. Something the user is, such as fingerprint, verified by biometric measurement

Objective

1. To protect Data confidentiality
2. To protect patient's Identity
3. User controlled read write access and revocation is the two main security objectives or concerns for any electronic health record model.
4. The main objective of our model is to grant secure patient-centric PHR access and efficient key management simultaneously.

Motivation

1. It is Integration of PHR with cloud service provides the following benefits: (1)Reduced cost, (2)Medical resource sharing and exchange, (3)Dynamic scalability of resources, (4)Enhanced flexibility, (5)Elimination of device limitation.
2. The proposed scheme for providing confidentiality and secure sharing of PHRs through the public cloud.

3. I made observation that People used PKE for Encrypting data. Due to the slower operations and the larger key sizes it becomes inefficient and then the SKE, PRE uses the same keys for encryption and decryption. But drawback of this scheme is, each file category is encrypted with distinct secret key so every time key needs to be provided whenever doctor tries to update file. Then ABE used for encryption that created bottleneck as computing load is heavy. Therefore there is need for implementation of new cryptosystem.

Problem Statement

A patient self-controllable multi-level privacy-preserving cooperative authentication in computing systems.An approach to resist various privacy attacks such as collusion attack, bruited force attack as well as SQL injection attack that can be performed while sharing PHR file by the patient/doctor to obtain the users security by encrypting file and Decrypting file and granting access permission to various user for PHR in cloud environment.

Input

1. Upload Medical Data information,
2. Register patient by Personal Information
3. Provide Access control mechanism

Output

1. File Encryption
2. Provide Generated Key
3. Download file
4. Secure Share of data and performance chart generated

Software Requirements

1. Operating system : Windows XP/7 onwards
2. Coding Language : JAVA, JavaScript
3. IDE : Netbean
4. Database : MYSQL

Conference and publication

1. Review paper A Methodology for Secure Sharing of Personal Health Records in the Cloud International Engineering Research Journal (IERJ), Volume 3 Issue 1 Page 4902-4904, 2018 ISSN 2395-1621

2. Paper presented at cpgcon 2019 Rathod V.U. and **Shaikh Aaliya**, The Privacy Based Secure Sharing Of Personal Health Records a Method in the Cloud, The 6th Post Graduate Conference of Computer Engineering (cPGCON-2019) 3rd -4th April 2019.

3. An Implementation paper Rathod V.U. and **Shaikh Aaliya** The Privacy Based Secure Sharing Of Personal Health Records a Method in the Cloud, Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162), JETIR1905E19 Volume 6 Issue 5 , May-2019

Project approach

In cloud computing, there are different existing techniques that provide security, data confidentiality and access control. Here users need to share their sensitive information with others based on the receivers ability to manage a policy in distributed systems. One of the encryption schemes is El-Gamal Encryption which is a new technique where such policies are termed and cryptographically enforced in the encryption algorithm itself.

Plan of Execution

COST AND TIME ESTIMATE: To achieve reliable costs and effort estimated, the estimation was delayed until late in the project and using one or more empirical models for software costs and effort estimates. Cost estimates must be providing up-front. However, we should recognize that longer we wait, the more we know and the less likely we are to make serious errors in our estimates. Cost estimation models can be used to completed decomposition techniques and oer a potentially valuable estimation approach in their own right. An estimation model for computer software uses empirically derived formulae to predict eort as a function of LOC (Line of code).For the estimation of software estimation was followed in the organic mode.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Cloud computing means storing and accessing data and programs over the internet instead of using computers hardware and software. Data security is the major problem in cloud computing. For security, different attribute based encryption schemes are used for encryption before outsourcing data to cloud server. Personal Health Record (PHR) service is an emerging model for health information exchange. It allows patients to create, update and manage personal and medical information. Also they can control and share their medical information with other users as well as health care providers. Advance technology of cloud computing PHR has undergone substantial changes. Most health care providers and different vendors related to healthcare information technology started their PHR services as a simple storage service. Then turn them into complicated social networks like service for patient to sharing health information to others with the emergence of cloud computing. PHR data is hosted to the third party cloud service providers in order to enhance its interoperability. However, there have been serious security and privacy issues in outsourcing these data to cloud server. For security, encrypt the PHRs before outsourcing. So many issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for clients data, a novel patient-centric framework is used.

1.1.1 Cloud Server

A cloud database is a collection of content, either structured or unstructured, that resides on a private, public or hybrid cloud computing infrastructure platform. Two cloud database environment models exist: traditional and database as a service (DBaaS).In a traditional cloud model, a database runs on an IT department's infrastructure via a virtual machine. Tasks of database oversight and management fall upon IT staffers of the organization.

What is Database as a Service? By comparison, the DBaaS model is a fee-based subscription service in which the database runs on the service provider's physical infrastructure. Different service levels are usually available. In a classic DBaaS arrangement, the provider maintains the physical infrastructure

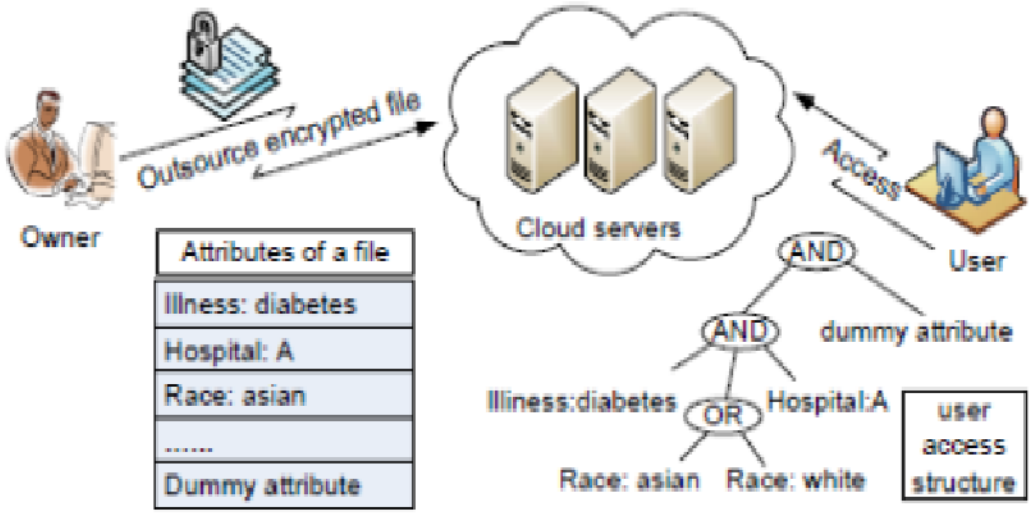


Figure 1.1: Privacy preserve secure sharing of PHR data

and database, leaving the customer to manage the database's contents and operation.

Alternatively, a customer can set up a managed hosting arrangement, in which the provider handles database maintenance and management. This latter option may be especially attractive to small businesses that have database needs, but lack the adequate IT expertise.

Cloud database benefits Compared with operating a traditional database on an on-site physical server and storage architecture, a cloud database offers the following distinct advantages:

Elimination of physical infrastructure: In a cloud database environment, the cloud computing provider of servers, storage and other infrastructure is responsible for maintenance and availability.

1.1.2 PHR:Personal Health Record

A personal health record (PHR) is simply a collection of information about a persons health. It is a tool for the excellent management of the health. Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records has proposed a scheme in which a file can be uploaded without key distribution and it is highly efficient. But it is a single data owner scenario and thus it is not easy to add categories. Shared and Searchable Encrypted Data for un trusted Servers, has explored that the data encryption scheme does not require a trusted data server. There is concern about security issues when outsource these data to the cloud server. Surveys show that seventy five percentage people are not choosing PHR system because they are concern about the security issues. For secure storing better method for designing PHR system is based on encryption method. Before outsourcing data to the third party different encryption methods are used. Public key Encryption (PKE) based scheme is one of the encryption method used for protecting data from third parties. But it has high key management overhead, or requires encrypting multiple copies of a file using different users keys. Attribute based encryption is based on some access policies. These access policies are expressed based on the attribute

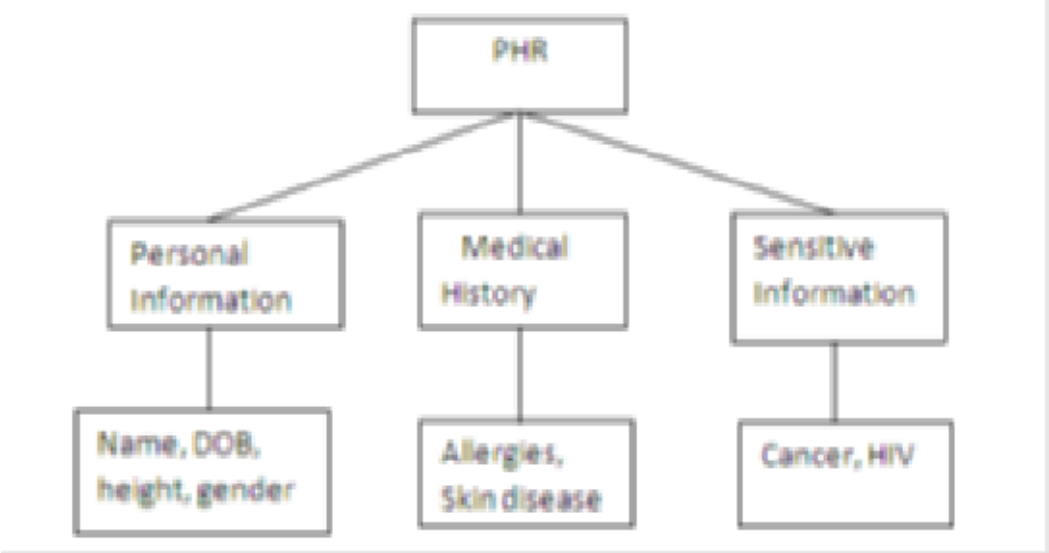


Figure 1.2: PHR information divided

of users or data which help to share PHR among set of users by encrypting the file under a set of attributes. Only authorized users with satisfying this access policy can access the PHR data. . The organization that owns and operates the database is only responsible for supporting and maintaining the database software and its contents. In a DBaaS environment, the service provider is responsible for maintaining and operating the database software, leaving the DBaaS users responsible only for their own data.

Although the transfer of PHR to cloud environment greatly increases security threats, data integrity, confidentiality, and availability cannot be compromised either. Since the primary objective of the PHR system is to grant lawful access to authorized users, we realize this objective through cryptography. Following is a brief introduction to cryptography and encryption systems. Cryptography is a practice and study of techniques (such as mathematical formulas) to randomize messages in order to render them unreadable to other users. By encrypting messages from plaintext into ciphertext, important messages can be protected. Private Key cryptosystem is also known as symmetric cryptosystem or one-key cryptosystem. In this system, the plaintext is encrypted and decrypted with one single private key. Prior to sending the message, the sender consults with the receiver over the private key to be used. Following, the sender encrypts the message with the private key into cipher text and sends it to the receiver. Upon receiving, the receiver uses the same private key to interpret the cipher text into plaintext for reading. Figure 2 illustrates the process. Symmetric key sizes are typically 128 or 256 bitsthe larger the key size, the harder the key is to crack. For example, a 128-bit key has 340,282,366,920,938,463,463,374,607,431,768,211,456 encryption code possibilities. As you can imagine, a brute force attack (in which an attacker tries every possible key until they find the right one) would take quite a bit of time to break a 128-bit key. Whether a 128-bit or 256-bit key is used depends on the encryption capabilities of both the server and the client software. SSL Certificates do not dictate what key size is used.

Figure 1.3: Private Key Cryptosystem

Public key cryptosystem is also known as asymmetric cryptosystem, or two-key cryptosystem. In this password system, two different keys are used for encryption and decryption, them being the receiverspublic key and the corresponding private key respectively.A complex mathematical relation exists between the two keys to ensure no one can derive the private from the public key within a limited time. Public key cryptography has the following advantages: (1)Protects information privacy, (2)Simplifies allocation and management of keys, (3)Possess non-repudiation. Although public key password system have the abovementioned advantages, owing to complex encryption and decryption processes, its efficiency is generally low. Though larger keys can be created, the increased computational burden is so significant that keys larger than 2048 bits are rarely used. To put it into perspective, it would take an average computer more than 14 billion years to crack a 2048-bit certificate.

Since asymmetric keys are bigger than symmetric keys, data that is encrypted asymmetrically is tougher to crack than data that is symmetrically encrypted. However, this does not mean that asymmetric keys are better. Rather than being compared by their size, these keys should compared by the following properties: computational burden and ease of distribution.

Symmetric keys are smaller than asymmetric, so they require less computational burden. However, symmetric keys also have a major disadvantageespecially if you use them for securing data transfers. Because the same key is used for symmetric encryption and decryption, both you and the recipient need the key. If you can walk over and tell your recipient the key, this isnt a huge deal. However, if you have to send the key to a user halfway around the world (a more likely scenario) you need to worry about data security.

Asymmetric encryption doesnt have this problem. As long as you keep your private key secret, no one can decrypt your messages. You can distribute the corresponding public key without worrying who gets it. Anyone who has the public key can encrypt data, but only the person with the private key can decrypt it. Pre-shared key encryption (symmetric) uses algorithms like Twofish, AES, or Blowfish,

to create keysAES currently being the most popular. All of these encryption algorithms fall into two types: stream ciphers and block ciphers. Stream ciphers apply a cryptographic key and algorithm to each binary digit in a data stream, one bit at a time. Block ciphers apply a cryptographic key and algorithm to a block of data (for example, 64 sequential bits) as a group. Block ciphers are currently the most common symmetric encryption algorithm.

1.2 Problem Statement

A PHR system where there are numerous PHR owners and PHR users. The owners could be patients who have full access control over their own PHR data where they can construct/generate, maintain and delete it. There is a server which belongs to the PHR service provider which stores all the owners PHRs. The users may come from various fields; for example say a friend, a guardian or a researcher. Following are the 3 phases:

1.3 Disadvantages of Existing System

- Prevention of Unauthorized Users Access: It is an important requirement for efficient PHR access is to enable patient-centric sharing. This means that the patient should have all the control over their personal health record.
- Fine Grained Access Control : Fine grained access control should be used in a manner that different users are authorized to read different sets of documents. Whenever a users attribute is no longer applicable, the user need not be able to access further PHR files using that same attribute.
- Attribute Revocation : The PHR system should allow users from both the personal domain and public domain. Considering the groups of end users from the public domain may be immense in size and uncertain, the system should be scalable, in managing the complexity in key management, communication, computation and storage too. Provide the security from insider attacks like collusion attack, bruited force attack as well as SQL injection attack.

1.4 Need of Project

Main issues are in the case of emergency department. In work flow based access control scenarios, the data access right could be given based on users identities rather than their attributes, while existing does not handle that efficiently. If a person is admitted to emergency department after the emergency treatment they tried to find out the medical records of that person. Using break glass access ED can access data. But they cannot refer other department or other doctor because their file is encrypted using some attributes i.e. Emergency department, Physician or other type of specialized doctors. This is the main drawback of the practical implementation of the system. In existing system work flow based conditions are not checked.

Chapter 2

LITERATURE SURVEY

Several recent studies have focused on the issue of secure sharing of electronic health records in the cloud.

S. Yu, C. Wang, K. Ren, and W. Lou, Achieving secure, scalable and fine-grained data access control in cloud computing, ,[1]:

In this system, the issues of concurrently achieving the fine-grained access, scalability, and confidentiality of the outsourced data are addressed. The data encrypted by a single owner is subsequently shared with multiple users by distributing the keys. To enable data owner to delegate the computational tasks to the untrusted cloud servers, the access policies based on the attributes are enforced. To deal with the heavy computation overheads caused by re-encryption of data files and update of secret key, the KP-ABE, PRE, and lazy re-encryption are combined But the management of multiple keys by the PHR owners, which eventually leads to overheads at the PHR owners end. Thus the security threat persists in to existing system.

Kuo-Hsuan Huang, En-Chi Chang, and Shao-Jui Wang, A Patient-Centric Access Control Scheme for Personal Health Records in the Cloud,[2]:

This paper proposed a scheme for patient-centric access control over PHR data. The proposed scheme ensures the following security properties: (1) confidentiality of health data, (2) integrity of health data, (3) authenticity of health data, (4) patient-centric fine-grained access control, and revocation of access control using symmetric key cryptosystem and proxy re -encryption (PRE) scheme. But the main drawback of this scheme is, each file category is encrypted with distinct secret key so whenever a data user (e.g. Doctor or nurse) wants to update PHR categories,

patient have to provide the corresponding secret keys. Besides this, the scheme is based on proxy re-encryption scheme which requires data owners to have too much trust on the proxy that it only converts cipher texts according to his instruction. A PRE scheme allows data owners to delegate to the proxy the ability to convert the cipher texts encrypted under his public key into ones for data users. Hence it is desired that proxy doesn't reside in the storage server. This increases communication overhead since every decryption requires separate interaction with the proxy.

So in this paper, shows redesign the scheme in [2] for patient-centric access control over PHR data belonging to the patient using the concept of a key-aggregate cryptosystem. Our solution ensures the following security properties: (1) confidentiality of personal health data, (2) integrity of personal health data, (3) authenticity of personal health data, (4) patient -centric fine-grained access control, and (5) revocation of access control.

[4] Chen, Y. Y., Lu, J. C., Jan, J. K. A secure EHR system based on hybrid clouds, [4]:

In this paper, proposed an EHR solution, relying mainly on smart cards and RSA that enables patients to store their medical records on hybrid clouds. In this approach, patients medical records are stored in two types of cloud: the hospitals private cloud and the public cloud. The authors discussed two usage cases. The first is that of the medical records being accessed by the owner of the data, i.e., the doctor who created the records. They can directly access the records from their private cloud or from the public cloud. The authors also provide a solution for emergency situations. However, the shortcoming of this approach is that data owners, i.e., doctors have access control for the medical records and their computing load is heavy.

Leng, C., Yu, H., Wang, J., Huang, J. Securing Personal Health Records in the Cloud by Enforcing Sticky Policies, [5]:

This paper proposed a solution that allows patients to specify a policy to support fine -grained access control. They primarily utilized Conditional Proxy Re- Encryption to enforce sticky policies and provided users with write privileges for PHRs. When users finish writing data to their PHRs, they sign the modified PHRs. However, users sign the PHRs using the signature key of the PHR owner and it is therefore difficult to correctly verify who signed the PHRs.

T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, Secure Dynamic access control scheme of PHR in cloud computing, [6]:

In this paper The health records are encrypted and decrypted through Lagrange multipliers using the SKE. The approach allows the data owners to generate and share the keys. An important feature of the approach is automatic revocation of the users. Allows multiusers to access PHRs simultaneously

Drawback Is High implementation overheads in cloud also in Semi- trusted servers poor audit However, the task is costly in terms of computations

J. Pecarina, S. Pu, and J.-C. Liu, SAPPHIRE: Anonymity for enhanced control and private collaboration in healthcare clouds, [7]:

In this paper Introduces anonymity boundaries between the user and provider. The patients encrypt the PHRs by the patients through the public key of the Cloud Service Provider (CSP) and the CSP decrypts the record using the private key, stores the health record and the location of the file (index), and subsequently encrypts them through the symmetric key encryption Drawback However, a limitation of the approach is that it allows the CSP to de-crypt the PHRs that in turn may act maliciously.

[8] D.H Tran, N. H.-Long, Z. Wei, N. W. Keong, Towards secu-rity in sharing data on cloud-based social networks, [8]:

In this paper a secure framework for data sharing among users of a group. This framework provides the keyword search function that help users query on the groups data based on pre-defined keywords . It allows the group administrator to easily revoke an user from the group. Since the keys are shared on both users and the proxy, once removed from the group, user is unable to access the groups data even though he still keeps his key.

Advantage: To enhance security, data is usually encrypted before sending to the servers. In this paper, we suggest a framework that allows users of cloud-based social networks to share their private data in a secure manner.

In our framework, every user in a group has his own secret key to encrypt and decrypt data. The key will be revoked if the user leaves the group. Using proxy re-encryption schemes, the framework helps any user be able to access others data in the same group.

Drawback : The Key Manager should be a third-trusted party which share data with proxy there can be theft or malicious during sharing Therefore, if the proxy re-encryption scheme is semantically secure, the proxy cannot know any information from any users data. The major threat in the framework is the collusion between the proxy and one of the users, even with a user who have left the group. If this collusion occurs, based on the keys distributed from the key manager, the proxy can disclose all other users key. For instance, let say user j has left the group. He now colludes with the proxy to reveal others key. Another important issue is the work load on the proxy which may suffer too many encryption or decryption operations.

Chapter 3

DISSERTATION PLAN

3.1 Introduction

The PHR is logically partitioned into the following four portions:

1. Personal Information
2. Medical information
3. Insurance related information
4. Prescription information

However, it is noteworthy that the above said partitioning is not inflexible. It is at the discretion of the user to partition the PHR into lesser or more number of partitions. The PHRs can be conveniently partitioned and can be represented in formats, for example XML. Moreover, the PHR owner may place more than one partition into same level of access control. Any particular user might not be granted a full access on the health records and some of the PHR partitions may be restricted to the user

A researcher might only need the ac-cess to the medical records while deidentifying the personal details of the patients. The access rights over different PHR partitions are determined by the PHR owner and are delivered to the SRS at the time of data uploading to the cloud.

3.2 Project Schedule

Project planning emphasizes on following aspects:

1. Work Breakdown:Load the Work Breakdown Structure data into the planning and scheduling repositories. As the Work Breakdown Structure content is derived, progressively load the data into the planning and scheduling repositories. Generate reports, review the content and progressively update the data. This process continues on an iterative basis. Hierarchical Tree of activities and outcomes.

2. Make work statement for each task: The project schedules show the timing and sequence of tasks within a project, as well as the project duration and consist of tasks, dependencies among tasks, durations, constraints, milestones and other time oriented project information. The schedules specify the relative beginning and ending times of activities and their occurrence times.

3. Above shows the Plan of Project that will be the basis for the execution and tracking of all the project activities, which is used throughout the life of the project and kept up to date to repect the actual accomplishments and plans of the project.

4. Requirement Analysis and study part of the project was as follows: Understanding the problem definition; Understanding the current scenario in Market; Gathering information about required Software; Gathering information about required Software Resources; Preparing preliminary design of overall work flow of project; Deciding the modules required for overall execution.

5. 5. The schedules may be presented on a calendar framework or on an elapsed time scale. For the individual project being planned, the Work Breakdown Structure and task dependencies are used to develop estimates, resource allocations and an initial critical path prior to integrating it with other work

6. Streams and optimizing the overall schedule

7. Responsibilities and involvement.

8. Budget and time estimates: 9. Means that the duration assigned to the task remains fixed whether the resources assigned to the task are increased or decreased. As a result, the change in resources will change the tasks work eort requirement.

9. The selection of the appropriate category depends upon whether the duration of the task can be shortened by assigning more resource to it. Duration is defined as the total span of working time required to complete a task.

10. Duration is defined as the total span of working time required to complete a task. To estimate project length, the approximate elapsed time for each task is calculated using the formula: Phase or Rolling Wave Planning.

11. In larger projects, it may be acceptable to consider the entire project at a high level and only perform detailed planning and scheduling for one or two stages of the project at a time. This may result in a more accurate short term view and may save rework in correcting information at a later stage in the light of less uncertainty. This is often referred to as Phase or Rolling Wave Planning.

12. We have created system in java. Data is stored in mysql database. We have created a web application with local server. Web application that communicates with local server and Trustee Server .We have uploaded text document on cloud. We have evaluated this system of PHR of patient used to the hospitals.

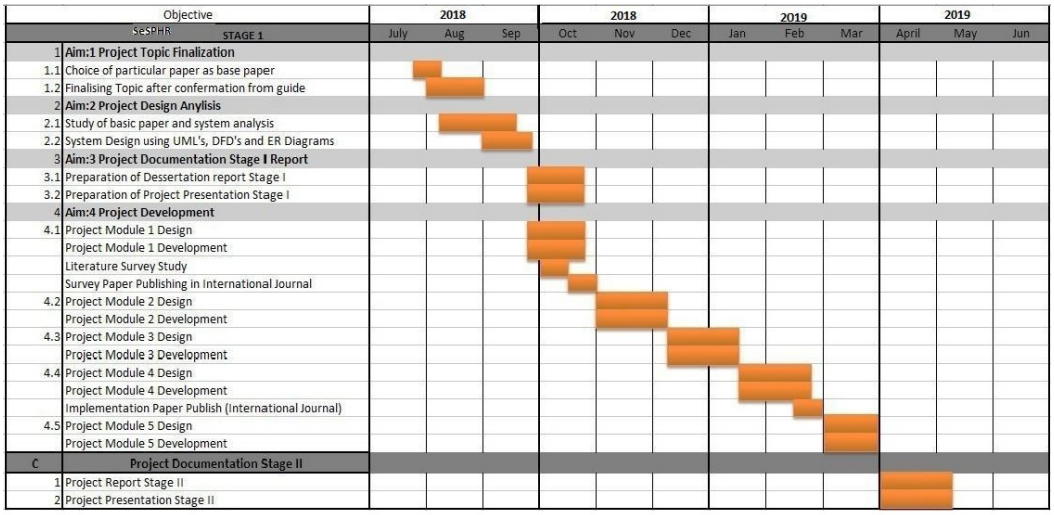


Figure 3.1: Planning procedure

13. Here we also calculate the file each file size for analysis purpose.

14. More Security and Easily -deployed solution for encryption that supports PHR Data

15. User Friendly: Use command-line client that supports

16. esolve the problem of access control of health record

3.3 System Implementation Plan

Delivery Date	Target	Description
Jul 2018	Requirement Gathering	Literature survey for domain selection
Aug 2018	Analysis	Studying the scope of the problem, UML diagrams generate.
Sep 2018	Designing	Generating project GUI.
Oct 2018	Documentation	report with diagrams, SRS and assignments.
Jan 2019	Implementation	Implementation of Data and Link Extraction module
feb 2019	Coding	Coding of Feature Extraction module.
Mar 2019	Paper Publishing	Publishing a research paper
April 2019	Testing	System integration
May 2019	Complete	Completion of project

Table 3.1: Project Plan

Sr No	phase	activities
1	Study Analysis	This phase involves understanding of requirements and preparation of overall plan. 1 Studying the available literature 2 Identifying data sources for consumption data 3 Identifying integration nature of data 4 Identifying the final requirements
2	Domain Finalized	Decide the final Domain that work
3	Literature Research	Related work done for oblique right protected data
4	Problem Definition	Identify and Define Problem Definition
5	Project Title	Define Final Project Title
6	System Analysis	Critical analysis and comparison, results achieved in research.
7	Detail Design	identifying the hardware/software platforms to be used.
8	Planning Dataset	Modeling and design or Creation
9	Survey Paper	Published Paper on (IERJ)
10	Implementation	Implementation production environment. Prepare report
11	PHASE A	Implementation of Module-1
12	PHASE B	Implementation of Module-2
13	Module Testing	Test system quality, Test system for different datasets.
14	Final Report	Prepare
15	Final Presentation	Prepare

Table 3.2: PLAN OF DS

Chapter 4

PROBLEM DEFINITION AND SCOPE

4.1 Problem Definition

A system that can provide the security to Personnel Health Records (PHR) files using encryption as well as proxy re-encryption services, in cloud environment and provide the Security from insider attacks like collusion attack, bruited force attack as well as SQL injection attack. In cryptography, a collision attack on a cryptographic hash tries to find two inputs producing the same hash value, i.e. a hash collision.

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. When password-guessing, this method is very fast when used to check all short passwords, but for longer passwords other methods such as the dictionary attack are used because a brute-force search takes too long. a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

In short An approach to resist various privacy attacks such as collusion attack, bruited force attack as well as SQL injection attack that can be performed while sharing PHR file by the patient/doctor to obtain the users security by encrypting file Decrypting file and granting access permission to various

user for PHR in cloud environment.

4.1.1 Our Contribution

To define the a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamically to end user. Provide a secure way for key distribution with secure communication channels. The users can securely obtain their private keys from data owner. Scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked

4.2 Scope

The proposed methodology provides the following services for the PHRs shared over the public cloud.

1. o Identity Management
2. Authentication
3. Confidentiality;
4. Trust Management: Secure PHR sharing among the groups of authorized users
5. Policy Management : Securing PHRs from unauthorized access of valid insiders
6. Access Control : Backward and forward access control;
7. Compliance Management

I n the proposed methodology, the cloud is not considered a trusted entity. The features of cloud computing paradigm, such as shared pool of resources, multi tenancy, and virtualization might generate many sorts of insider and outsider threats to the PHRs that are shared over the cloud. Therefore, it is important that the PHRs should be encrypted before storing at the third-party cloud server. The PHR is first encrypted at the PHR owners end and is subsequently uploaded to the cloud. The cloud merely acts as a storage service in the proposed method-ology. The encryption keys and other control data are never stored on the cloud. Therefore, at the clouds end the confidentiality of the data is well achieved. Even if the unauthorized user at the cloud by some means obtains the encrypted PHR file, the file cannot be decrypted because the control data does not reside at the cloud and the confidentiality of the PHR is ensured.

Chapter 5

SYSTEM DEVELOPMENT

5.1 Block Diagram

5.2 Block Description

P ersonal Health Record is an internet based application that allows people to access and co-ordinate their lifelong health information and make if appropriate parts of its available to those who need. Personal Health Records security and protection of its data have been of great concern and a subject of research over the years. There are many different forms of cryptographic mechanisms like AES, MD5 proposed to guarantee data security. In this work we propose a unique authentication and encryption technique using AES algorithm. In PHR data refers to the information that is collected, analyzed and stored. Example: Medical history, List of medical problems, Medication history. The PHR owner herself should decide how to encrypt her file and to allow which set of users to obtain access to each file. In PHR infrastructure is the computing platform which processes or exchanges healthcare data such as software package and website.

5.2.1 (Patient) PHR Owner Module

The PHR Owner module provides secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains (PUDs) and personal domains (PSDs)) according to the different users data access requirements. This is patient registration module where details of patient provided and also suitable doctor is assigned to it. It also gives access control by requesting and distributing keys to different users.

5.2.2 Server Module

The server is semi-trusted. The system assumes each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols. In the framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users.

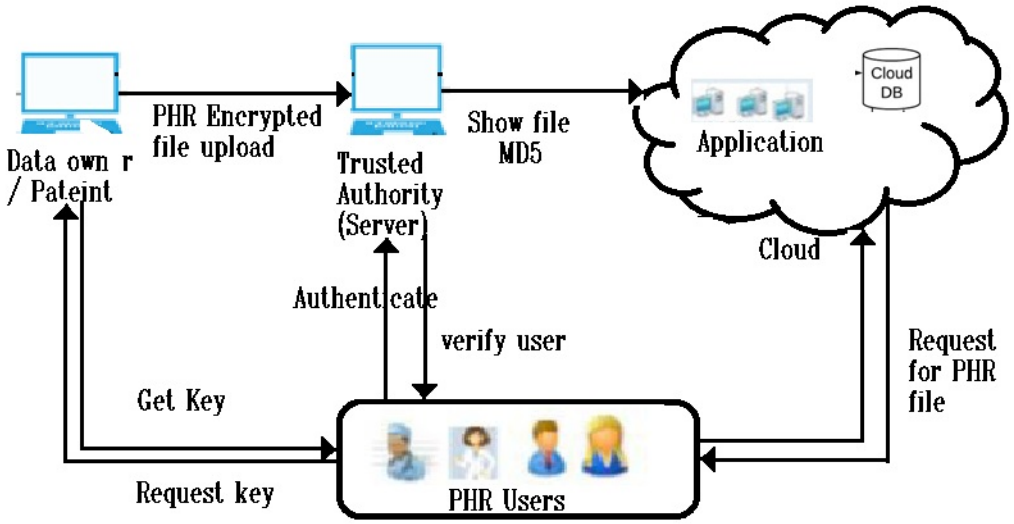


Figure 5.1: Existing System Block Diagram

5.2.3 Data confidentiality Module

The owners upload AES encrypted PHR files to the server. For encryption of AES algorithm and MD 5 technique is used for key generation technique is used for Encryption.

5.2.4 Doctor (PHR User)

This module takes user registration as doctor and assigned to patient on server authentication it can view patient file only on request granted and also provide prescription to patients based on it. Appointments are fixed and assigned to each patient are authorized.

5.2.5 Receptionist (PHR user)

This module provides appointment to doctor from patient. And have limited access to the data of patient .This shows how PHR system divided in different users but with separate domain access to each user.

5.2.6 cloud

On the cloud by the PHR owners for subsequent sharing with other users in a secure manner. The cloud is assumed as un-trusted entity and the users upload or download PHRs to or from the cloud servers. As in the proposed methodology the cloud resources are utilized only to upload and download the PHRs.

5.3 Methodology /Algorithms

A. Algorithm / Basic Steps:

1. Patient makes registration with email password phone and disease caused.

2. Admin or owner whenever makes login check the new user and activate them or deactivate them .
3. Doctor makes registration with email phone and specialization.
4. Admin or owner whenever makes login check the new user and activate them.
5. Patient is able to make login and update profile .
6. Patient makes request for appointment and submit details for doctor.
7. Receptionist makes registration and login.
8. Receptionist forward request to the doctor makes appointment fix.
9. The particular doctor is activated by admin and on login of that doctor is able to see request and patient disease
10. Then doctor uploads the file record of that patient in encrypted form.
11. Also precipitation is given to requested patient.
12. On patient login the file is download on key request.
13. If user is authenticated then email and text is sent of key for decryption.
14. user can now download file with key.
15. Analyses and prediction is seen by doctor login for more research and survey purpose

AES

AES is an Advanced Encryption Standard used for secure transmission of data that is personal health record in encrypted format. In our system AES is used for sending user authentication data n encrypted format. AES allows for three different key lengths: 128, 192, or 256 bits. For encryption, each round consist of the following four step:

Chapter 6

SOFTWARE REQUIREMENT SPECIFICATION

6.1 EXTERNAL INTERFACE REQUIREMENTS

6.1.1 User Interface

The user interface will be one of the standalone applications. User-friendly look and feel menus and screens are provided with easy access on a click of a button. We make the user interface using java, We follow the 3-tier architecture like DLL, BLL and UI, Behavioral pattern for design standard

6.1.2 Hardware Interface

No special hardware interface needed apart from standard personal computer. A computer that has enough hard disk space to board Operating System and enough processor speed to enable it to function normally is sufficient for developing the project.

6.1.3 Software Interface

The application will be developed using Web Browser as front-end Java, JSP and SQLSever as back-end. The Operating system used will be Windows.

6.1.4 Communication Interfaces

We use IP protocol for establishing connection and transmitting data over the network. We use local network for connecting the server.

6.2 SPECIFIC REQUIREMENTS

6.2.1 Functional Requirements

The code needs to be highly maintainable, as software engineering and design methodology is constantly evolving. If this software product is to be updated or maintained in a time and cost effective

manner, the code needs to be highly maintainable.

The performance of a number of functions is described as being interactive. This is defined as the user being able to get continuous and quick respond on the operation that they are performing. Resources should be provided so as to achieve required output.

6.2.2 Non Functional Requirement

Performance Requirements

To evaluate the performance and to check the obtained results following metric will be used:

1. Distortion Detection Accuracy
2. Classification Rate
3. Matching Accuracy
4. Performance will be measured based on confusion matrix such as precision and recall.
5. Both precision and recall are usually expressed as a percentage.

The project has the following performance requirements: The Product should be able to function 24x7. The client experience should be good and system should gives the expected output.

Technical feasibility study is the complete study of the project in terms of input, processes, output, fields, programs and procedures. It is a very effective tool for long term planning and trouble shooting. The technical feasibility study should most essentially support the financial information of an organization. Here we problem during the software installation with compatibility issues.

The purpose of an economic feasibility study (EFS) is to demonstrate the net benefit of a proposed project for accepting or disbursing electronic funds/benefits, taking into consideration the benefits and costs to the agency, other state agencies, and the general public as a whole. This system is benefit to all company, organization minimizing the attacks on server.

Performance Feasibility Study is an assessment of the practicality of a proposed project or system. This system is give the better graphical displays and calculates measures of performance. Proposed system performance is better than other, during detecting the unauthorized modification on database server.

Social feasibility is one of the feasibility studies where the acceptance of the people is considered regarding the product to be launched, this product once developed then we use the social use to the any company, organization, data centre, e commerce etc. for protecting the server attack from attacker.

Software Quality Attributes

Software Quality Attributes are the benchmarks that describe system's intended behavior within the environment for which it was built. The quality attributes provide the means for measuring the fitness and suitability of a product. Software architecture has a profound effect on most qualities in one way or another, and software quality attributes affect architecture.

1. Maintainability

   The system developing using Java framework, all are easy to modify and make update.

2. Portability

   This application is coding in java therefore, it should be transferable between different os.

3. Cost and Schedule

   The cost of the system with respect to time to market, expected project lifetime, and utilization of legacy systems.

4. Cost and Schedule

   The cost of the system with respect to time to market, expected project lifetime, and utilization of legacy systems.

6.3 HARDWARE AND SOFTWARE REQUIREMENT

6.3.1 Hardware Requirements

Architecture	32 Bit or 64 Bit
Processor	Pentium IV Processor or Above
RAM	2GB or Above
Hard Disk	100 GB and more

Table 6.1: Hardware Specification

Operating System	Windows 7,8
Software Development Phase	JDK 1.6.0 (JDK 7) Tomcat Apache Server
Techniques	Java, JSP
Databases	MySQL 5.0

Table 6.2: Software Specification

Chapter 7

Detailed Design Document

7.1 Mathematical Model

1. PHR Admin S = {p1,p2,d1,d2,r1,r2 }
    - p1 : Activate the registered patient for access control to view download file
    - p2 : Deactivate the registered patient for access control
    - d1: Activate the registered Doctor for access control to view upload file
    - d2: Deactivate the registered doctor for access control
    - r1: Activate the registered receptionist.
    - r2: Deactivate the registered receptionist.
2. Doctor: S2 ={ e1,e2,e3,e4,e5,e6,e7}
    - e1: Registration
    - e2: Login on activation and authentication
    - e3: View patient details
    - e4: View book appointments and grant permission request.
    - F1: Encryption using AES ()
    - F2: Encryption using MD5()
    - e5: upload encrypted file
    - e6 : provide key to mail on user request
    - e7: Add prescription
3. 3. Patient: S3=d1,d2,d3,d4,d5,T1,T2
    - d1: Registration
    - d2: Login on activation and authentication
    - d3: book appointment for checkup

- d4: View doctor information for appointment
- d5: View doctor provided precipitation
- T1:Request key and decrypt the AES file
- T2: Request key and decrypt the MD5 file.

4. Cloud or Server S3=s1,s2,s3,s4,s5,s6
    - s1: Authenticate Admin login
    - s2: Appointing particular doctor to patient request
    - s3: Store but cant view PHR files
    - s4:Sent key on request to particular patients mobile and email
    - s5: Make classification and analysis of doctor specialist present
    - s6: Also make prediction of diseases caused overall and gender prediction suffering form diseases.

1. **Success case:** Authentication successful doctor upload the file also patient able place appointment and to download the file decrypting under access control provided by admin.
2. **Failure case:** Details provided like email and phone number then key cant be received and no file will be accessed.

7.2 Algorithm

7.2.1 Algorithm 1: AES for Data Encryption

1. data block of 4 columns of 4 bytes is state
2. key is expanded to array of words
3. has 9/11/13 rounds in which state undergoes:
4. byte substitution (1 S-box used on every byte)
5. shift rows (permute bytes between groups/columns)
6. mix columns (subs using matrix multiply of groups)
7. add round key (XOR state with key material)
8. view as alternating XOR key, scramble data bytes
9. initial XOR key material incomplete last round
10. with fast XOR and table lookup implementation

7.2.2 Algorithm 2: AES Decryption

1. AES decryption is not identical to encryption since steps done in reverse
2. but can define an equivalent inverse cipher with steps as for encryption
3. but using inverses of each step with a different key schedule
4. works since result is unchanged when
5. swap byte substitution shift row
6. swap mix columns, add (tweaked) round key

7.2.3 Algorithm 3: MD5 Algorithm

1. Step 1: Arrange all input data D into the matrix Format and saved into the Log files.
2. Step 2: Consider a selected data m act as a new selected data.
3. Step 3: position m gets changed after allocated Time period.
4. Step 4: If data get hacked or leaked by some Malicious users.
5. Step 5: Data leakage occurs.
6. Step 6: To analyze the leakage data and Prevent using the data analysis (tamper Analysis).
7. Step 7: To get original data to call the revert Back function.
8. Step 8: When the user calls that dishonest file, hash Function gives to the user a previous Data. And log file maintained at the admin side.
9. Step 9: Return True.
10. Output - The hashed value is changed then the log will generate

7.3 Flowchart

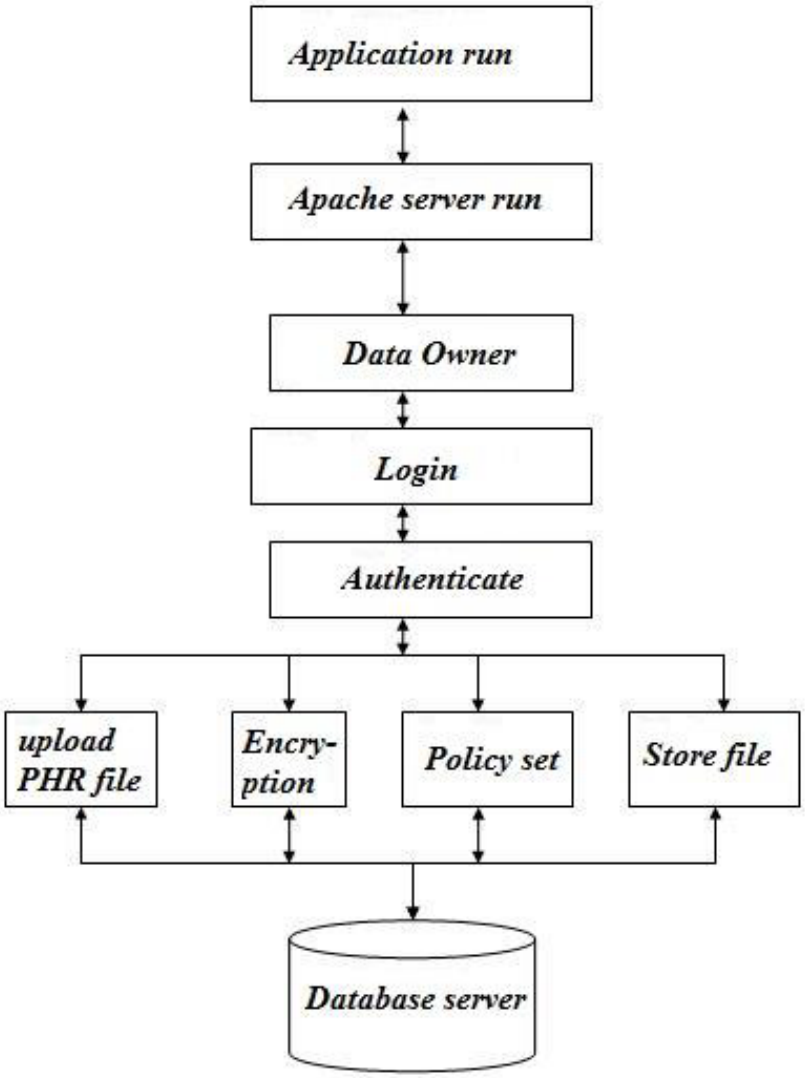


Figure 7.1: Flowchart

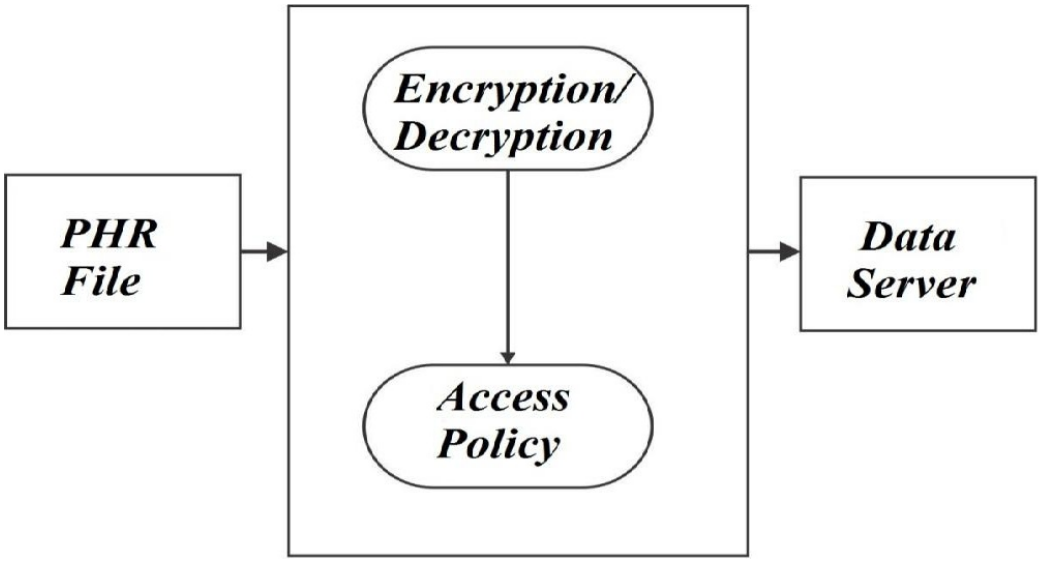


Figure 7.2: DFD level 0

7.4 UML Diagram

7.4.1 DFD Diagram

DFD is used to represent basic data flow of system, which provides addit0ional information helpful during analysis. DFD serves two purposes:

1.

2. 1. To provide an indication of data flow through the system.

3. 2. Pictorial representation of the functions and sub-functions that are used for transformation of data flow.

7.4.2 ER Diagram

This form of diagram is principally used to capture the relationships that exist between static data objects in a problem model or a design model. In particular, the Entity Relationship Model has provided an essential foundation for the development of the relational models that are used in many database systems

7.4.3 Class Diagram

The class diagram shows the structure of system by modeling the relation between different classes, their attribute, functions and objects. It is used to show the overview. of number of packages and classes in that different packages of the project. The relationship is denoted by logical connection between the classes and objects. Firth is login then option and the abou-us is havinf one to one relation.

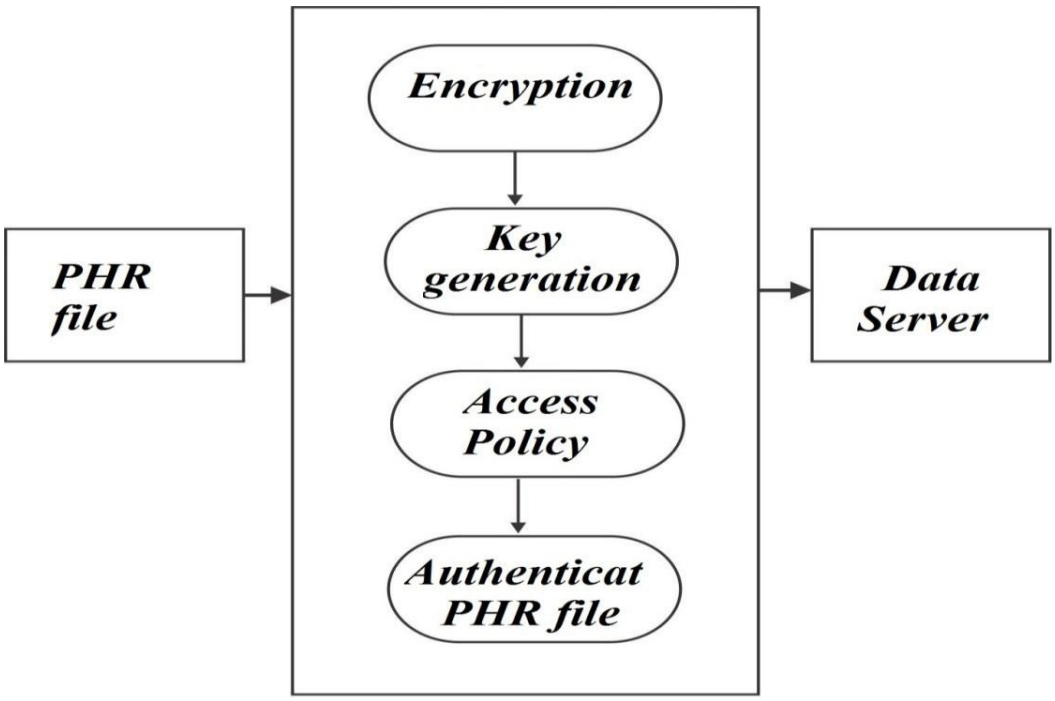


Figure 7.3: DFD level 1

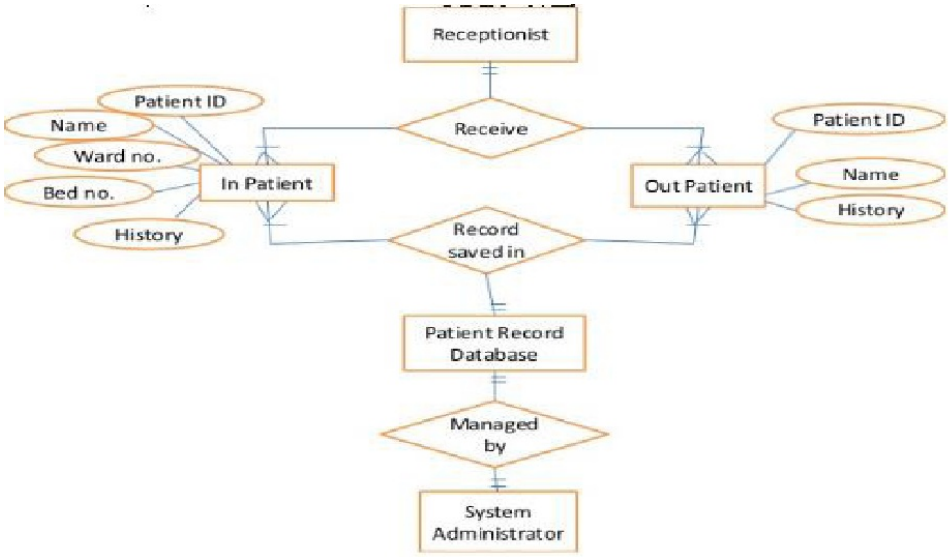


Figure 7.4: ER diagram

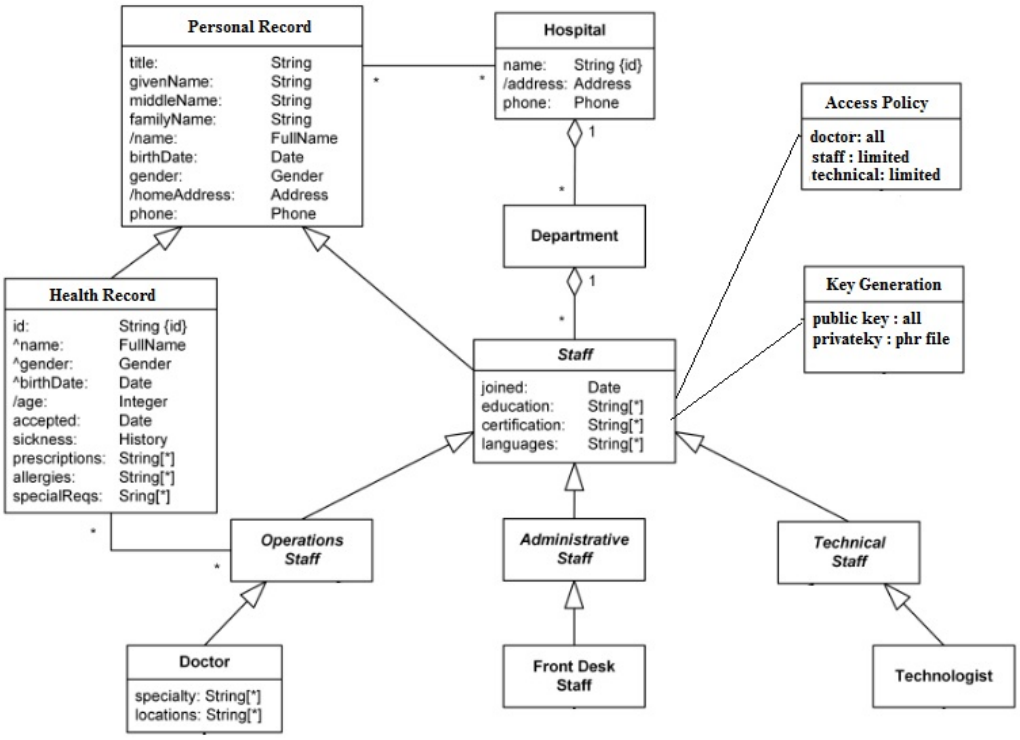


Figure 7.5: class diagram

7.4.4 Use case

Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. 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.

7.4.5 Activity Diagram

Activity diagrams can be used to describe the business and operational step-by-step workfl ow of components in a system. An activity diagram shows the overall flow of control. In this different activities of the system to be performed are explained as follows: 1. Add pateint by Registration 2. Login 3. Upload file and store it 4. Share and download file 5. Decrypt file

7.4.6 sequence Diagram

A sequence diagram shows object interactions arranged in time sequence. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario. Sequence diagrams typically are associated with use case realizations in the Logical View of the system under development. The Sequence Diagram models the collaboration of objects based on a time sequence. It shows how the objects interact with others in a particular scenario of a use case.

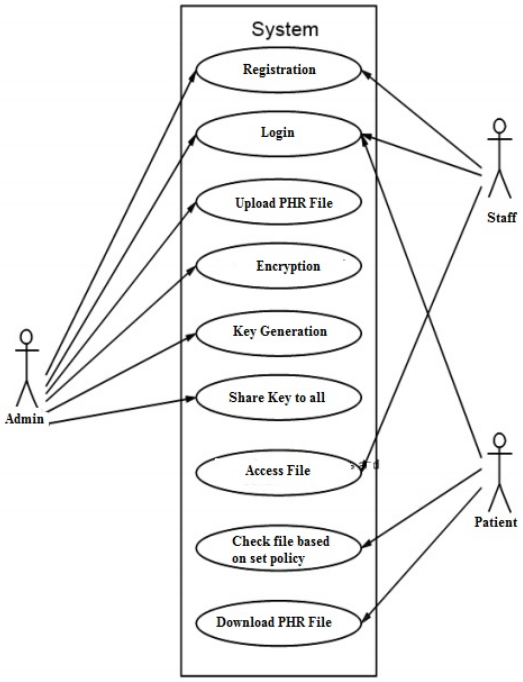


Figure 7.6: Use case

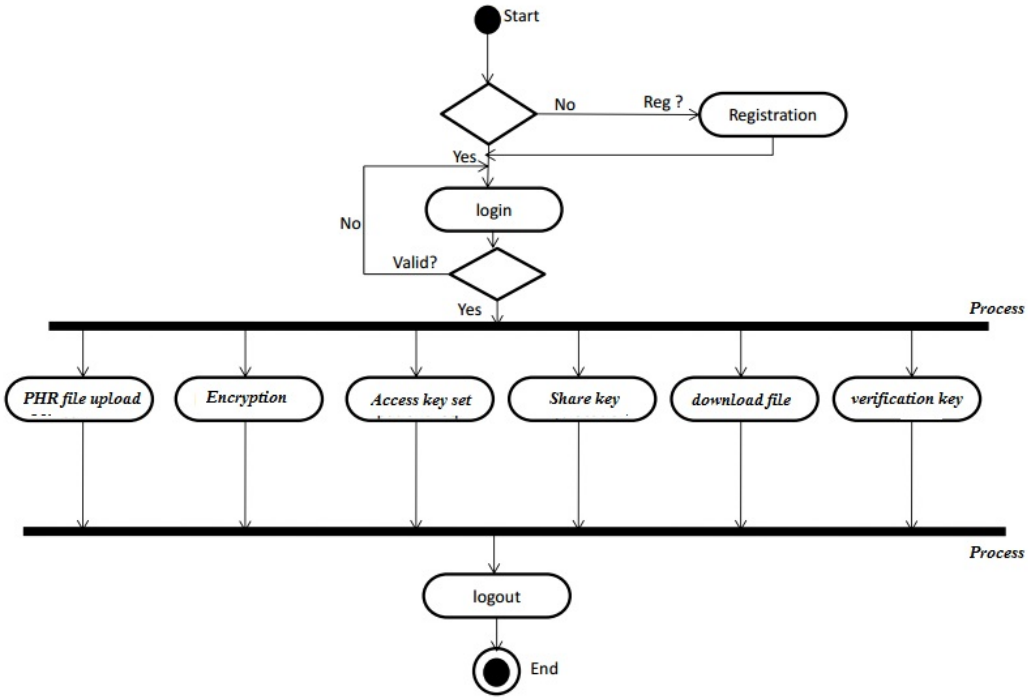


Figure 7.7: activity diagram

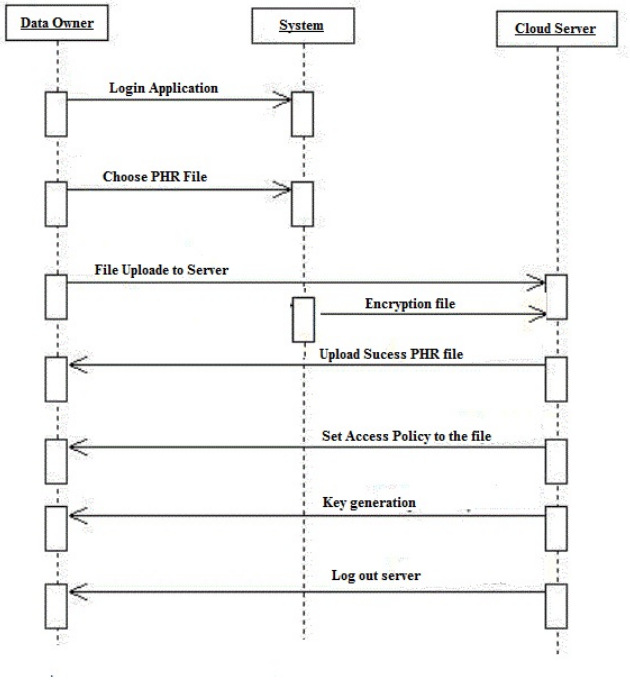


Figure 7.8: sequence Diagram

7.4.7 Component Diagram

This definition is interesting because it separates out two further supporting concepts, which are those of: 1. the component model that incorporates specific interaction and composition standards; and 2. the composition standard, that defines how components can be composed to create a larger structure. Expalin Reusability

7.4.8 collaboration Diagram

Above the links in a communication diagram are the numbered messages, indicating the order in which they are sent or received. The messages tell the receiver to perform an operation with specified arguments. Every communication diagram is equivalent to a sequence diagram, i.e., a communication diagram can be converted to an equivalent sequence diagram and vice versa. These two types of diagrams provide a message-oriented and time-oriented view, respectively.

7.4.9 Deployment Diagram

The basic deployment diagram element is the node. The node represents the environment in which a component or a set of components execute. This means that a node in a deployment diagram can represent a multitude of thingsphysical hardware such as a server machine, a system software like an operating system, or even application infrastructure software like a Web server, application server, database server, and so forth. The different nodes in the deployment diagram can be interconnected to represent interdependencies.

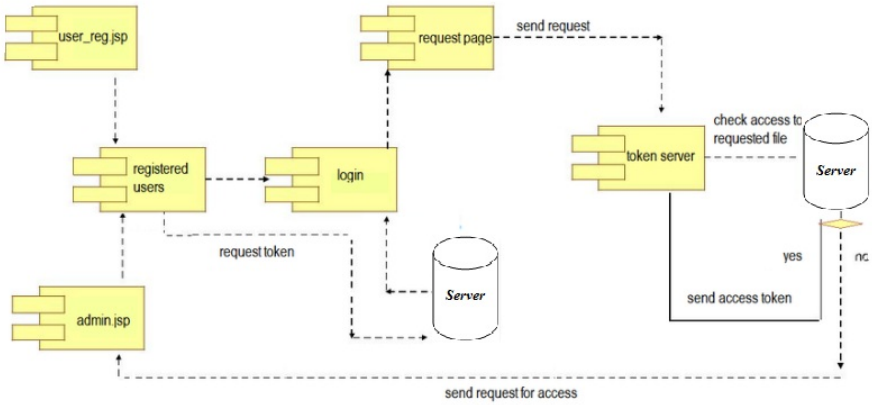


Figure 7.9: Component Diagram

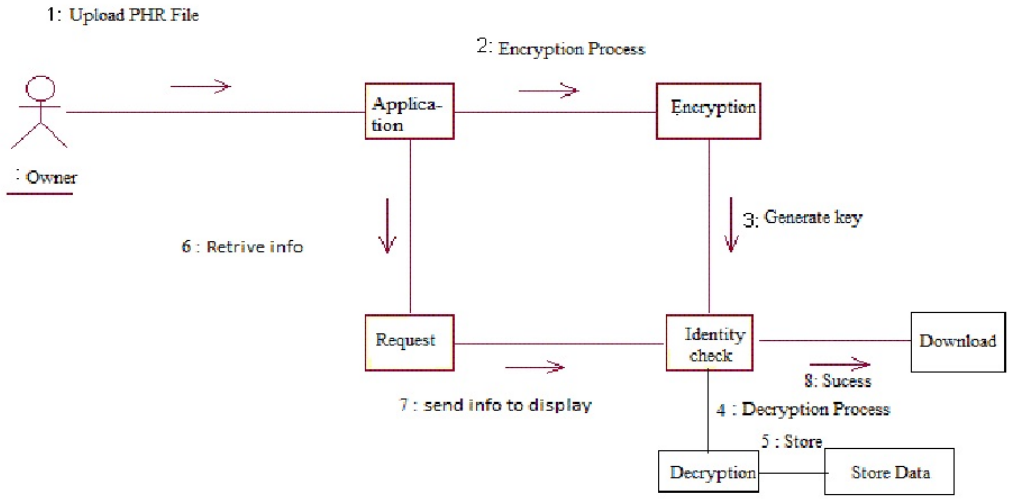


Figure 7.10: collaboration Diagram

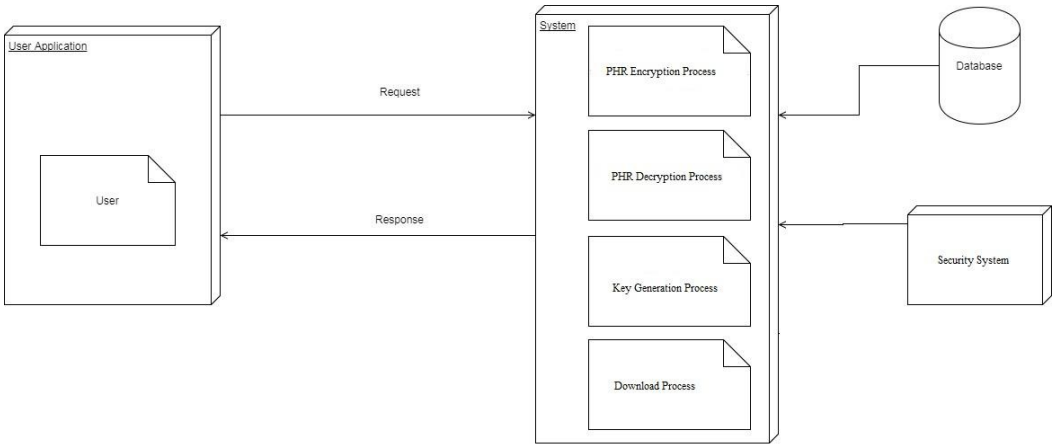


Figure 7.11: Deployment Diagram

Chapter 8

TEST SPECIFICATION

8.1 TEST CASES AND TEST RESULTS

Software testing is an important factor for the software quality Assurance and also represents the ultimate review of specification, design and code generation. Testing may include unit testing, integration testing, UI testing, Performance testing, system testing etc.

8.2 Type of Testing

Manual Testing or Automated Testing. Use Automated Testing Plan for planning automation activities in details. The different types of testing that may be carried out in the project are as follows:

1. Unit testing
2. Integration Testing
3. System Testing
4. Validation Testing
5. White Box Testing
6. Black Box Testing
7. GUI Testing

8.2.1 Unit testing

Individual components are tested independently to ensure their quality. The focus is to uncover errors in design and implementation, including Data structure in component , Program logic and program structure in a component, Component interface, Functions and operations of a component ,

8.2.2 Integration Testing

A group of dependent components are tested together to ensure their quality of their integration unit. This approach is to do incremental integration to avoid big-bang problem. That is when the entire program is put together from all units and tested as a whole. The big-bang approach usually results in chaos which incremental integration avoids. Incremental integration testing can be done in two different ways top down and bottom up.

8.2.3 System Testing

The system software is tested as a whole. It verifies all elements mesh properly to make sure that all system functions and performance are achieved in the target environment.

8.2.4 Validation Testing

Validation can be defined in many ways, but a simple definition is that succeeds when software functions in a manner that can be reasonably expected by the customer. Software validation is achieved through a series of black-box tests that demonstrate conformity with requirements. A test plan outlines the classes of tests to be conducted and a test procedure defines specific test cases that will be used to demonstrate conformity with requirements. Both the plan and procedure are designed to ensure that all functional requirements are satisfied

8.2.5 White Box Testing

This testing is concerned only with testing the software product; it cannot guarantee that the complete specification has been implemented.

8.2.6 Black Box Testing

Black box testing is concerned only with testing the specification; it cannot guarantee that all parts of the implementation have been tested. Thus black box testing is testing against the specification and will discover faults of omission, indicating that part of the specification has not been fulfilled.

8.2.7 GUI Testing

Because of reusable components provided as part of GUI development environments, the creation of the user interface has become less time consuming and more precise. But, the same time, the complexity of GUIs has grown, leading to more difficulty in the design and execution of the test cases. Because many modern GUIs have the same look and same feel, a series of test cases can be derived

Test case	1
Test Case Description	Register button show on home page of application
Steps	1.Click on the Register button. 2. Registration page should get open.
Test case result	After clicking on the Register button of the system should perform the respective operation.
Action Result	After clicking on the Register button of the system should perform the respective operation.
Status	Pass

Table 8.1: Test case registration

Test case	2
Test Case Description	Login button show on home page of application application
Steps	1.1.User fill the User ID and password in text Box button. 2. User click on LogIn Button
Test case result	Login Successfully
Action Result	Login Successfully
Status	Pass

Table 8.2: Test case Login

Test case	3
Test Case Description	System should Verify Password and Username
Steps	User should click on OK button for verification
Test case result	Fail
Action Result	failed
Status	success if usernmae password incorrect

Table 8.3: Authentication

Test case	4
Test Case Description	Upload the encrypted file
Steps	3 select file to upload 4.Click on submit button
Test case result	After clicking on the submit button of system should perform the encryption.
Action Result	After clicking on the submit button of system should perform the encryption.
Status	pass

Table 8.4: Upload file

Test case	5
Test Case Description	Request for key
Steps	5. For user click on download file it request for key. 6. User receives mail or text of key.
Test case result	After clicking on the Download button of the system should perform the respective operation.
Action Result	After clicking on the Download button of the system should perform the respective operation.
Status	Pass

Table 8.5: File key Request

Test case	6
Test Case Description	Download on decryption of file
Steps	7. User enter the the key. 8. Clicking on add key file is decrypted now user is free to download
Test case result	After clicking on the Add key button of the system should perform decryption the respective operation.
Action Result	After clicking on the Add key button of the system should perform decryption the respective operation.
Status	Pass

Table 8.6: Decryption of file

Chapter 9

RESULT AND DISCUSSIONS

The web app;ication created on cloud based on health care system. To manage , store and share data on cloud. Using cryptosystem files uploaded are encryted and decrypted using Advance encryption system and Message digest algorithms.

We propose a sensitive policy; privacy based approach to the PHR files sharing.

1. For minimizing the loss of the uploaded files from unauthorized patient/user.
2. For minimizing the disclosure risk.
3. To maintain the diversity among the uploaded PHR files.
4. Minimized security on files on sharing sites.

The performance of this method based on the access policy set to each PHR file which is shown in Table 1 for different access policy result is successful. The Encryption /Decryption time, Key generation and total time of process should be minimum for good performance.The result is to meet expected output on given experimental data file. The system Privacy Based Secure Sharing Of Personal Health Records a Method in the Cloud that needs to upload patients information in encrypted form on cloud with policy set on cloud and that file is decrypted with key based on authentication also policy based access.

The expected result is to generate key, encryption of file with secure storage on cloud to avoid misuse of information some accessibility rights are set and key is provided based on that to guarantee confidentiality. Also valid system user cannot obtain the re-encryption parameters for a PHR partition for which access is not granted to the user. The server gives user access permission and keys to user. The Actual output works with patient registration and login also patient upload PHR file and set policy send on doctor desk for checking. The PHR file is encrypted before uploading. Decryption done with key asked from user firstly policy is checked the key provided for decryption of data.

9.1 Gender prediction

Sr No	pateint name	file name	Access policy	Result
1	Jhon	NeurotherapyTreatemnt.doc	Doctor,pateint	success
2	peter	Hearttreatement	Doctor ,pateint	Success
3	ganesh	DailyTreatment	Receiptionist	Success
4	Linda	Tablets plan	Receiptionist	Success

Table 9.1: Access policy set to phr file

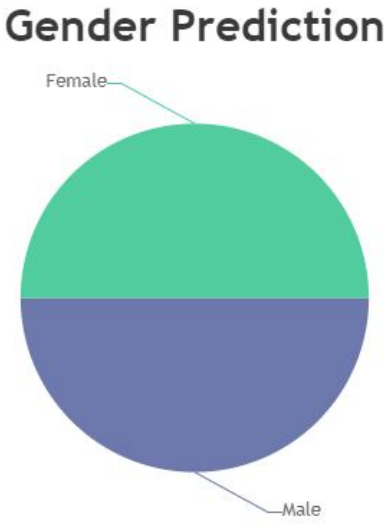


Figure 9.1: No of male female with disease

Gender	Percent
Male	50
Female	50

Table 9.2: Gender prediction for curing

File name	File Size	Existing System (encryption in sec)	Proposed System (encryptionin sec)
Abc.txt	80kb	4sec	2sec
Xyz.txt	100kb	6sec	4sec
Pqr.txt	150kb	8sec	6sec
Report.txt	300kb	15sec	12sec

Table 9.3: Encryption Process Time In Existing System And Proposed System Different File Size

This returns the time required for encryption using this technique.

upload.JPG

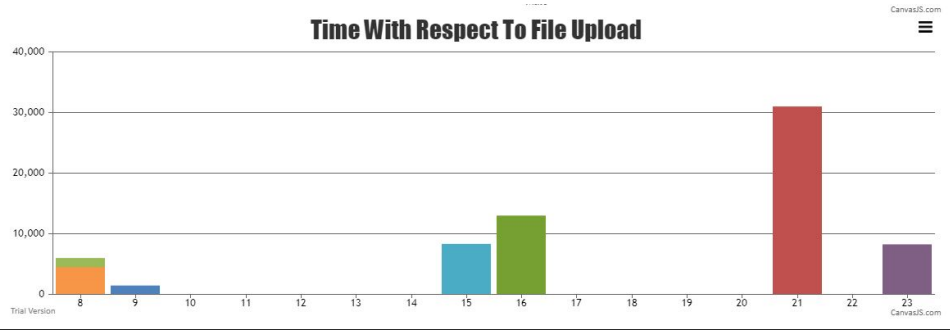


Figure 9.2: Encryption time graph

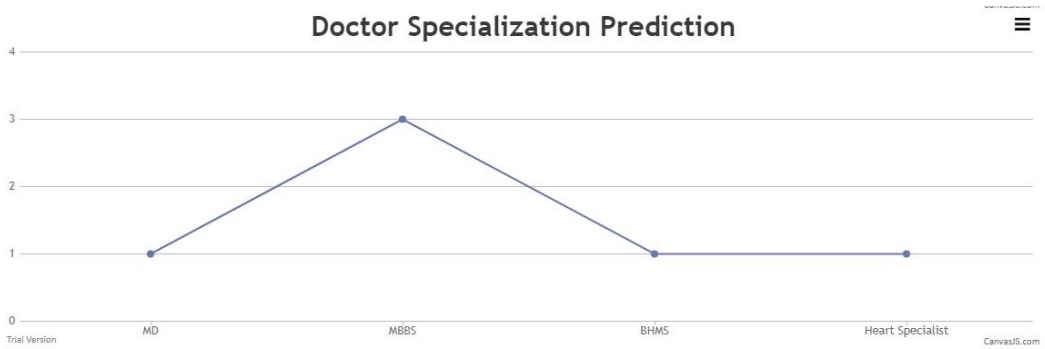


Figure 9.3: Doctor Specialization

SrNo	Specailist(x axis)	Number of present(y axis)
1	MD	1
2	MBBS	3
3	BHMS	1
4	Heart	1

Table 9.4: Doctor specialization in hospital

This graph table shows number of doctor in particular special field in hospital for further improvement.

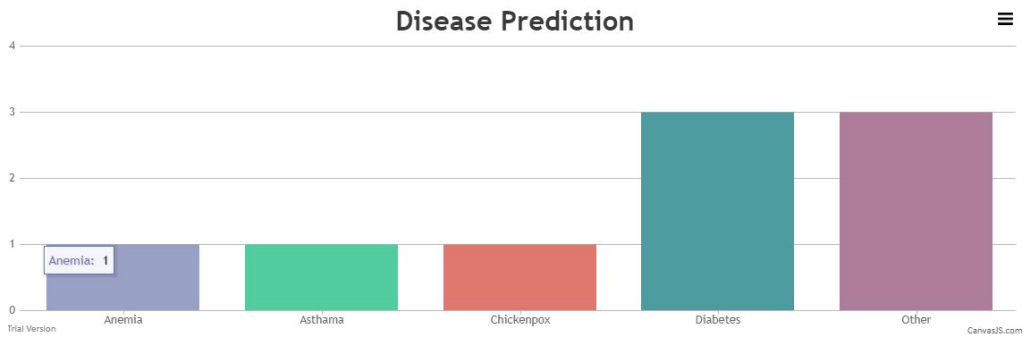


Figure 9.4: Disease Prediction

SrNo	Diseases(x axis)	Number of present(y axis)
1	Asthma	1
2	Anemia	1
3	chikenpox	1
4	Diabetes	3
5	Others	3

Table 9.5: Disease Prediction in hospital

This graph shows the number of patient with particular diseases are grouped together using bayes classification. Hospital maintains the record on this survey for further improvement in management.

9.2 Screenshots

Homepage where homepage with admin login , doctor login , patient login, receiptionist login is present.

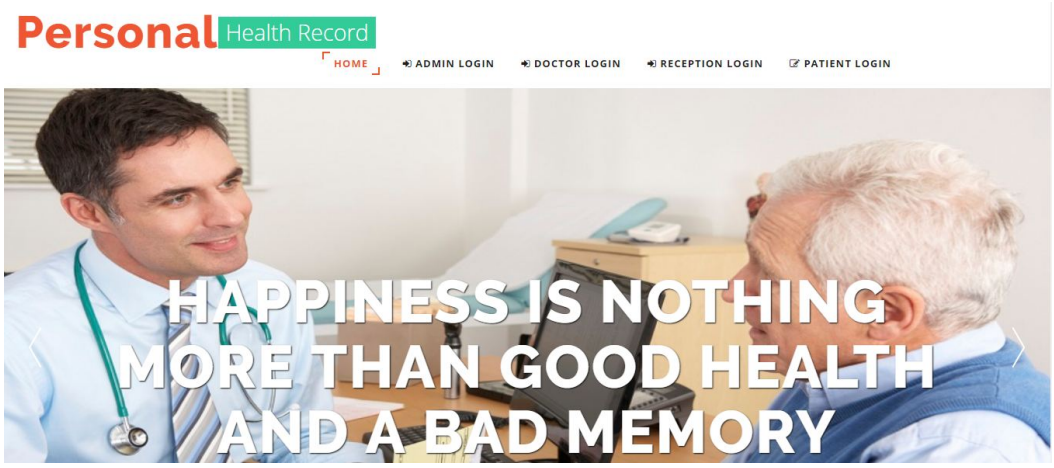


Figure 9.5: Homepage

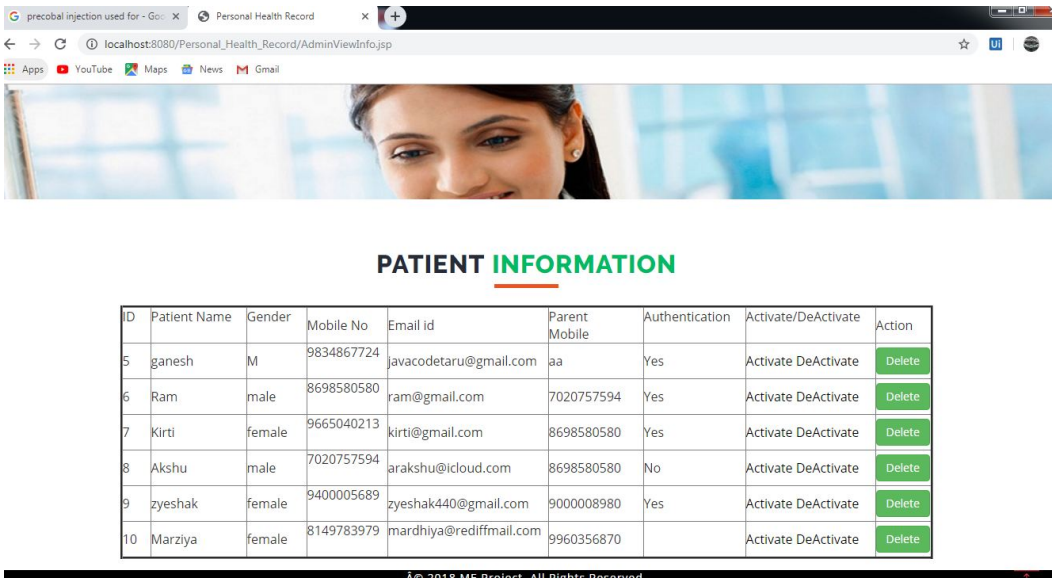


Figure 9.6: Admin page VIEW PATIENT AND DOCTOR:

Admin log-in and admin page where patient info and doctor info is shown in form of list appointments there activated or deactivated .

Admin log-in and admin page where Doctor info.

DOCTOR INFORMATION

ID	Doctor Name	Mobile No	Email id	Specialization	Experience	Authentication	Activate/DeActivate	Action
2	Akshu	7020757594	arakshu@icloud.com	MD	2 Year	Yes	Activate DeActivate	Delete
3	Ganesh	8888888888	javacodetaru@gmail.com	Heart Specialist	4 Year	Yes	Activate DeActivate	Delete
4	Kirti	9999999999	kirti@gmail.com	MBBS	1 Year	Yes	Activate DeActivate	Delete
5	Tausif	7894561230	tausif@gmail.com	BHMS	1 Year	Yes	Activate DeActivate	Delete
6	Akshay	8698580580	akshu@gmail.com	MBBS	2 Year	Yes	Activate DeActivate	Delete
7	Aalia shaikh	8237870768	aaliashaikh1395@gmail.com	MBBS	1 Year	Yes	Activate DeActivate	Delete

Figure 9.7: Doctor information shown to admin for activation:

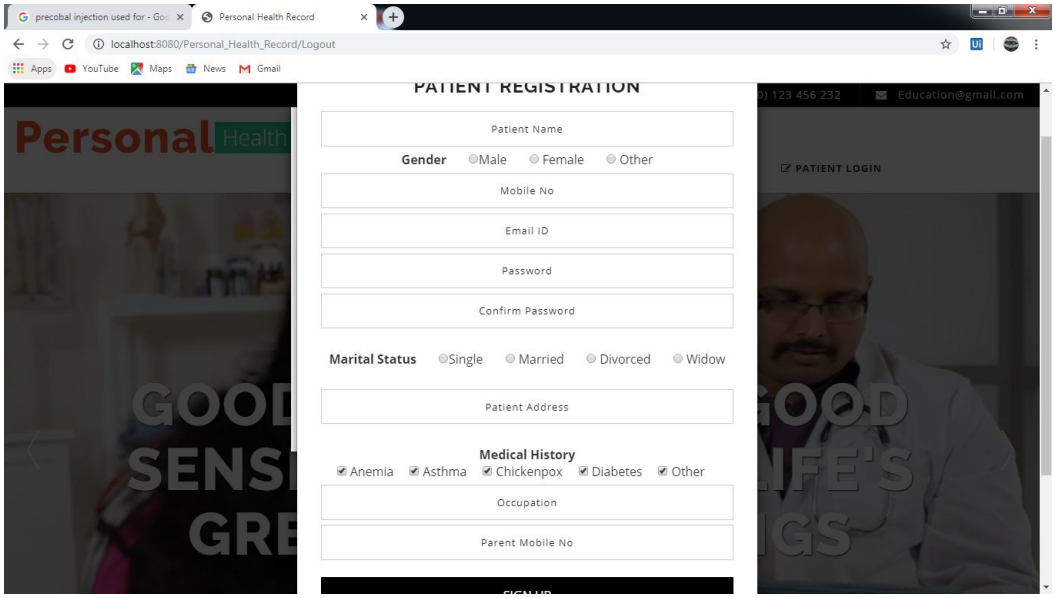


Figure 9.8: Patient registration page

Patient can register with following details.

Doctors can register with following details.

Encrypted file is uploaded from doctor side regarding treatment and other personal details of patient that is related to past information of patient.

Patient view the uploaded encrypted file of doctor giving treatment details in it

Admin log-in and admin page where Doctor info.

Encrypted file is viewed and can only be downloaded using its key so entering right key will download the file

Encrypted file is downloaded using its key so entering right key will download the file

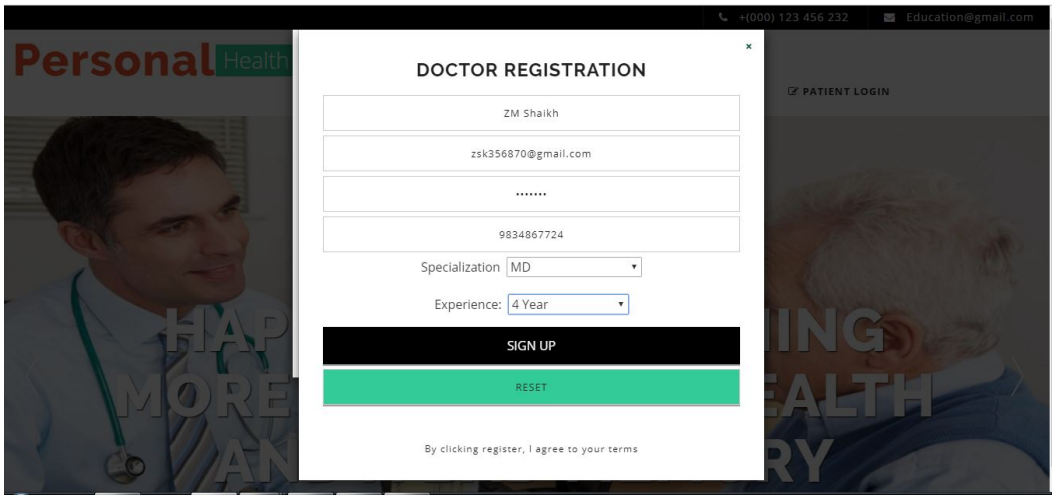


Figure 9.9: Doctor Registration

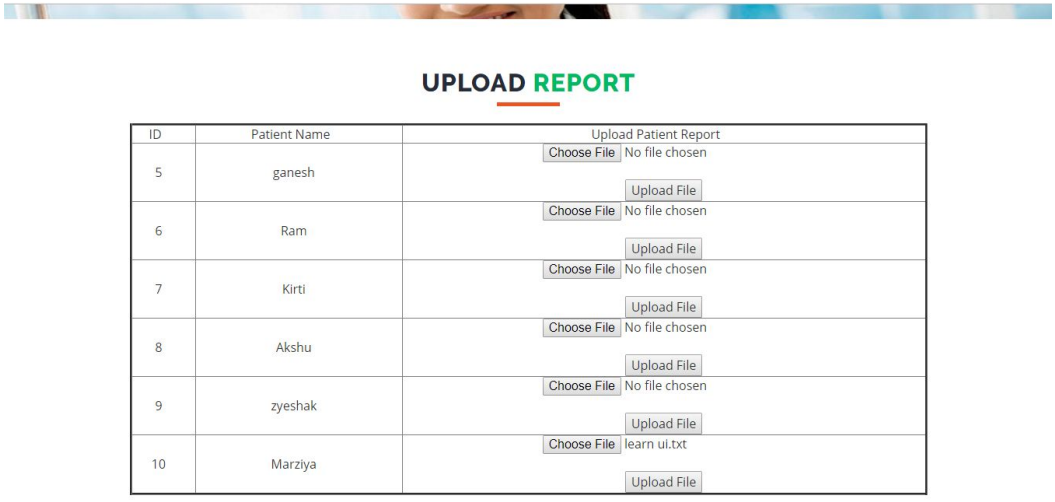


Figure 9.10: Doctor upload file

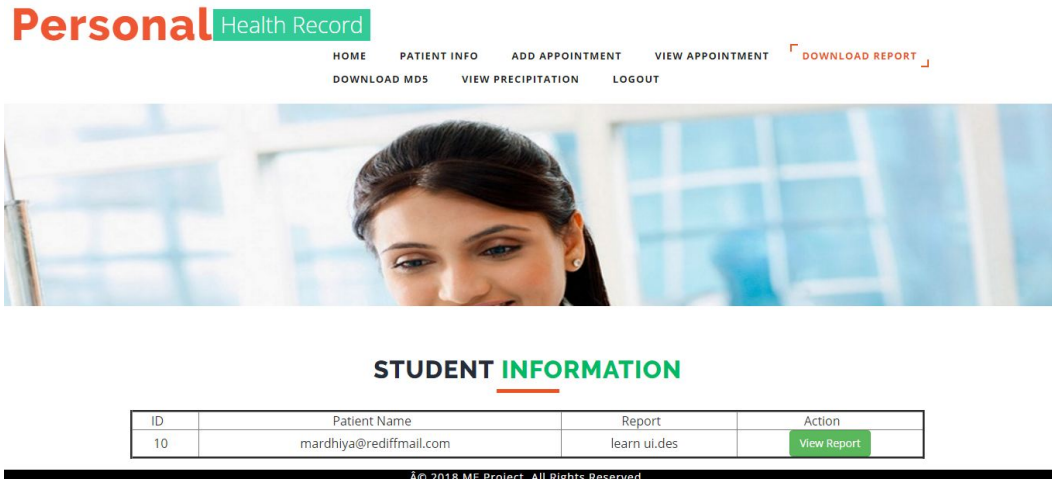


Figure 9.11: view encrypted report to patient from doctor uploaded

DOCTOR INFORMATION

ID	Doctor Name	Mobile No	Email id	Specialization	Experience	Authentication	Activate/DeActivate	Action
2	Akshu	7020757594	arakshu@icloud.com	MD	2 Year	Yes	Activate DeActivate	Delete
3	Ganesh	8888888888	javacodetaru@gmail.com	Heart Specialist	4 Year	Yes	Activate DeActivate	Delete
4	Kirti	9999999999	kirti@gmail.com	MBBS	1 Year	Yes	Activate DeActivate	Delete
5	Tausif	7894561230	tausif@gmail.com	BHMS	1 Year	Yes	Activate DeActivate	Delete
6	Akshay	8698580580	akshu@gmail.com	MBBS	2 Year	Yes	Activate DeActivate	Delete
7	Aalia shaikh	8237870768	aaliashaikh1395@gmail.com	MBBS	1 Year	Yes	Activate DeActivate	Delete

Figure 9.12: Doctor information shown to admin for activation:

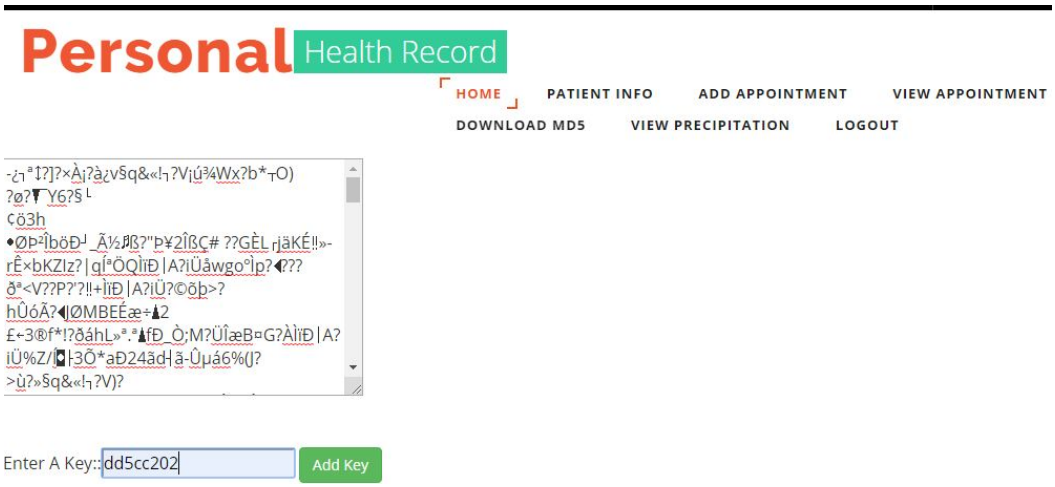


Figure 9.13: Encrypted file using AES technique

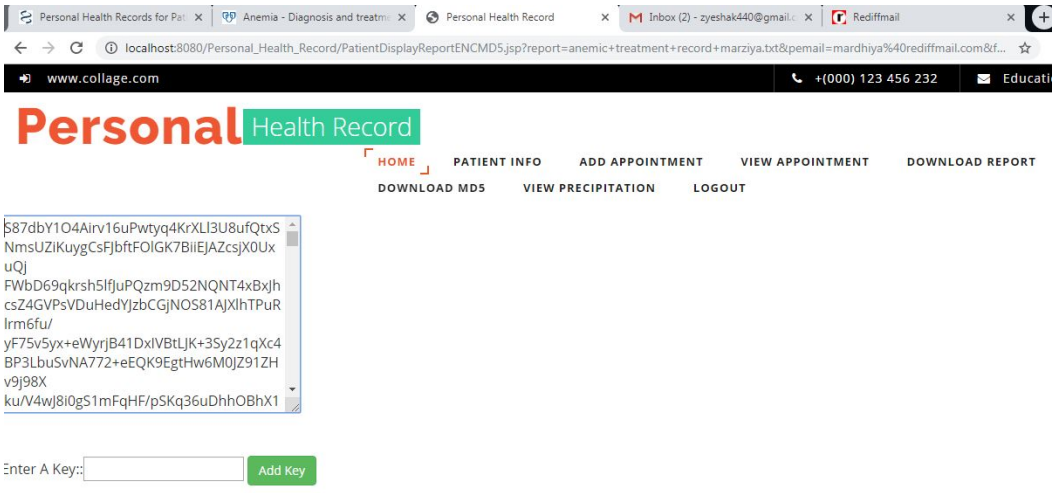


Figure 9.14: Encrypted file using MD5 technique

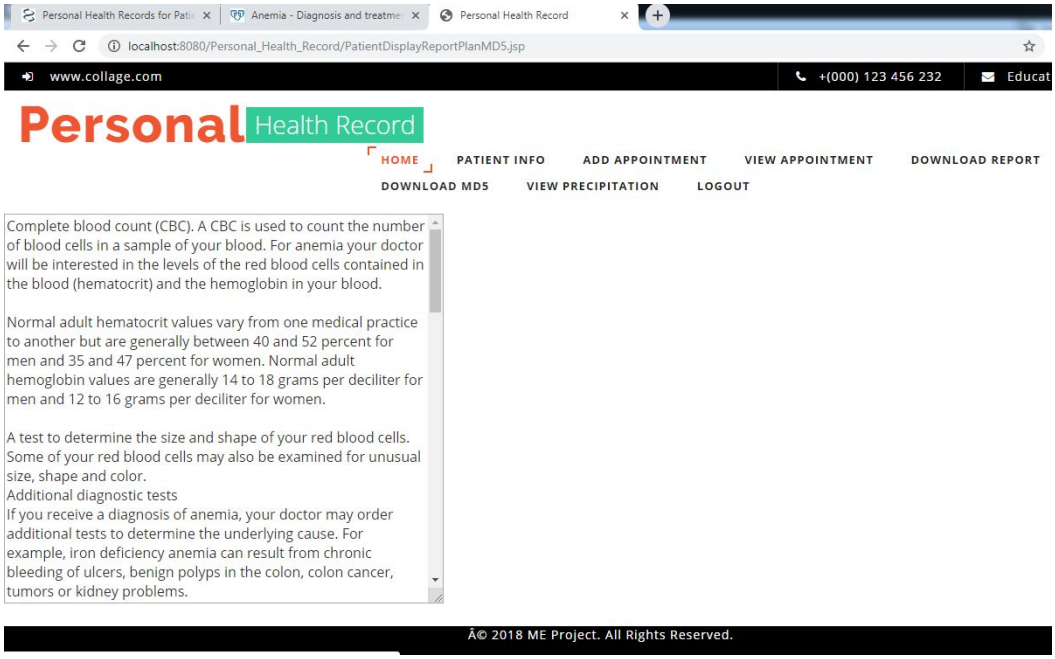


Figure 9.15: Download file

Registration of Receptionist so that admin can authenticate and patient can place appointment.

Patient have placed their appointment time and date that is approved by receptionist.

Doctor provide the list of medicines for patient.

Patient receive following list of medicine on login.

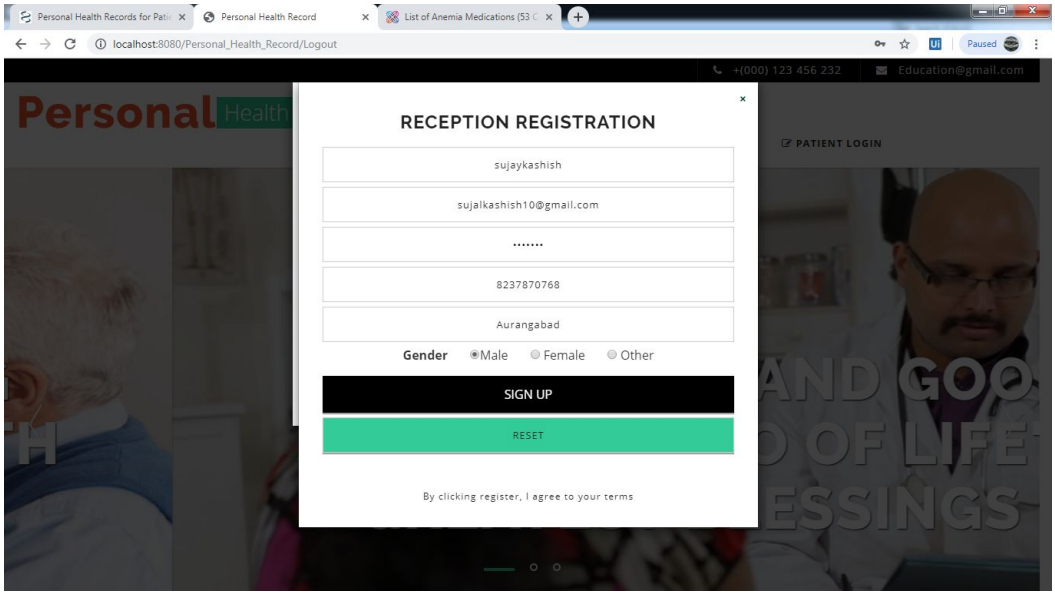


Figure 9.16: Registration of Receptionist

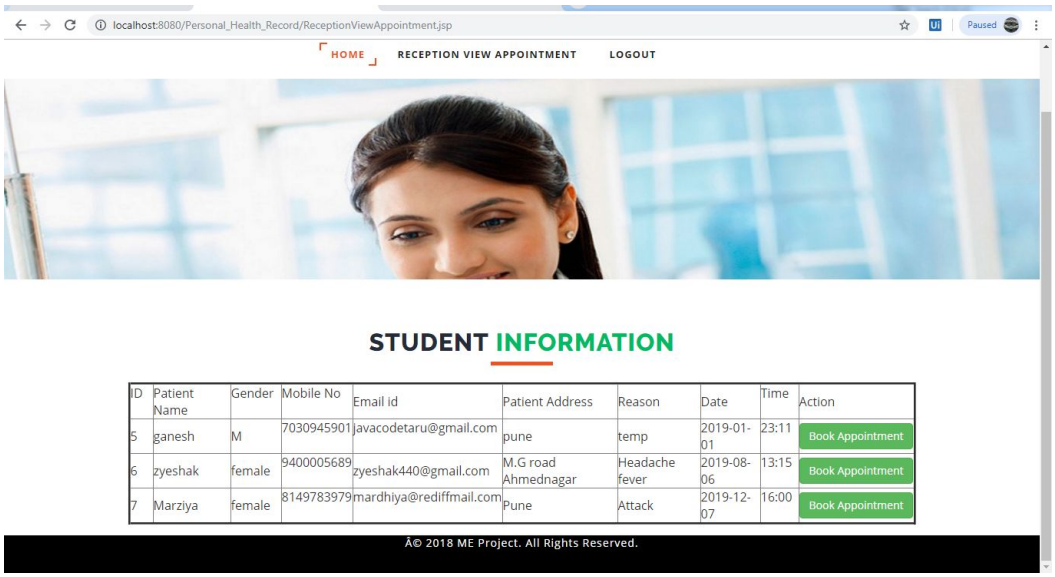


Figure 9.17: List of Appointments

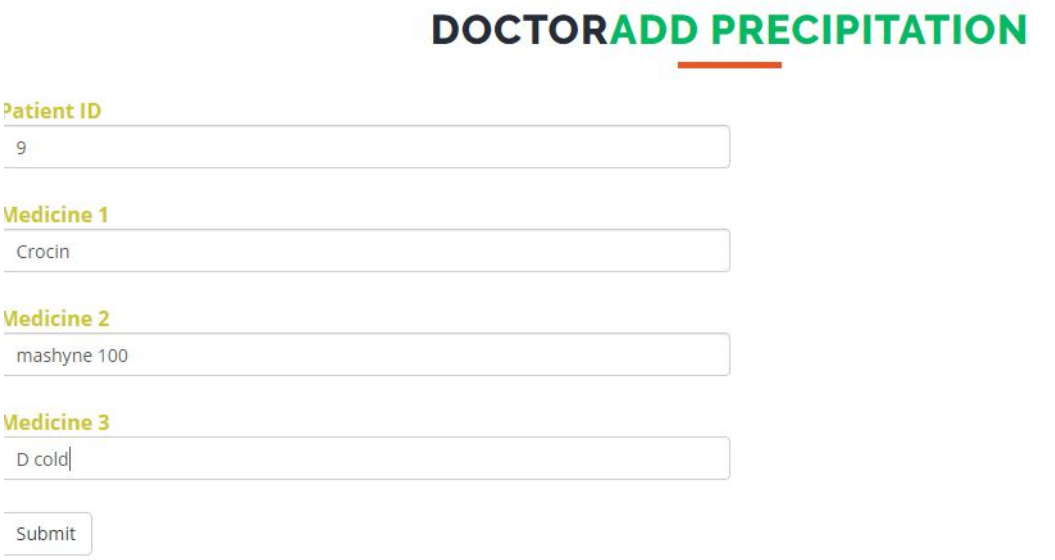


Figure 9.18: Doctor add prescription to patient

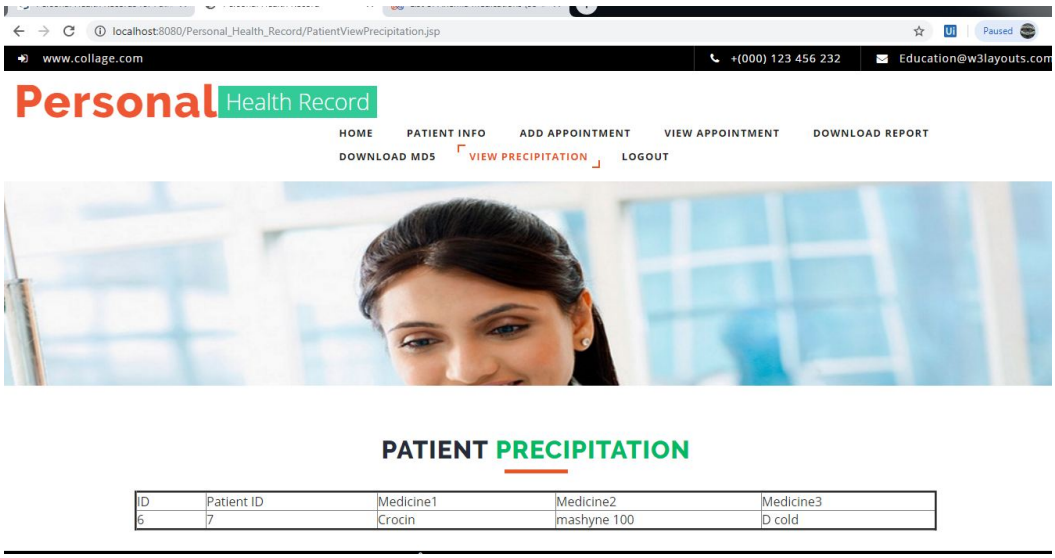


Figure 9.19: Prescription of patient

9.3 Discussion

9.3.1 Advantages

1. The advantages of our scheme are Confidentiality of Personal Health Data.
2. Authenticity of Personal Health Data.
3. Patient-centric fine-grained access control.
4. Allow user to efficiently manage their data.
5. Quickly find out information of patient details.
6. In case of emergency doctor and other emergency department quickly get all the details all the informative details and start treatment.
7. If in any condition doctors and medical facilities are not available the PHR owner itself able to take care of his health.
8. To provide easy and faster access information.
9. To provide user friendly environment.

9.3.2 Limitation

1. The proposed system disadvantages is if the server get fail uploading time then file will not analysis and no upload to the server.

9.3.3 Application

1. Government hospital private record
2. Private hospital data server
3. Health insurance
4. Any organization can use this application to store their employees medical information.

CONCLUSION AND FUTURE SCOPE

This methodology preserves the confidentiality of the PHRs and enforces a patientcentric access control to different portions of the PHRs based on the access provided by the patients. Thus a finely Grained access access control method in such a way that even the valid system users cannot access those portions of the PHR for which they are not authorized. The PHR owners store the encrypted data on the cloud and only the authorized users possessing valid re-encryption keys issued by a semi-trusted proxy are able to decrypt the PHRs. The role of the semi-trusted proxy is to generate and store the public/private key pairs for the users in the system. In addition to preserving the confidentiality and ensuring patient-centric access control over the PHRs, the methodology also administers the forward and backward access control for departing and the newly joining users, respectively. Moreover, we formally analyzed and verified . The performance evaluation was done on the on the basis of time consumed to generate keys, encryption and decryption operations, and turnaround time.

FUTURE SCOPE

In futhure studies we will look into machine learning techniques using automated system for providing more efficient health care system. If consider different credential are equal then Distributed ABE scheme is needed. We also this project work on real time application using the hospital record based on global server.

Bibliography

[1] S. Yu, C. Wang, K. Ren, and W. Lou. *The Achieving secure, scalable and fine-grained data access control in cloud computing.* in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-99

[2] Kuo-Hsuan Huang, En-Chi Chang, and Shao-Jui Wang *A Patient-Centric Access Control Scheme for Personal Health Records in the Cloud.* Fourth International Conference on Networking and Distributed Computing, 2014.

[3] Dixit, G. N *Patient Centric Frame Work For Data Access Control Using Key Management In Cloud Server.* International Journal of Engineering, 2 (4), 2013

[4] Chen, Y. Y., Lu, J. C., Jan, J. K. *A secure EHR system based on hybrid clouds.* Journal of medical systems, 36 (5), 3375 -3384, 2012.

[5] Leng, C., Yu, H., Wang, J., Huang, J. *The Securing Personal Health Records in the Cloud by Enforcing Sticky Policies.* in TELKOMNIKA Indonesian Journal of Electrical Engineering, 11 (4), 2200-2208, 2013.

[6] T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin *Secure Dynamic access control scheme of PHR in cloud computing.* in Journal of Medical Systems, vol. 36, no. 6, pp. 40054020, 2012.

[7] J. Pecarina, S. Pu, and J.-C. Liu. *The SAPPHIRE: Anonymity for enhanced control and private collaboration in healthcare clouds.* in Proceedings of the 4th IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 2012, pp. 99106.

[8] S. Yu, C. Wang, K. Ren, and W. Lou. *The Achieving secure, scalable and fine-grained data access control in cloud computing.* in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-99

[9] D.H Tran, N. H.-Long, Z. Wei, N. W. Keong *The Towards security in sharing data on cloud-based social networks.* in 8th In-ternational Conference on Information, Communications and Signal Processing (ICICS), 2011, pp. 1-5.

[10] Ming Li, Shucheng Yu, and Yao Zheng *The Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption.* in IEEE Transactions on Parallel and Distributed Systems, 24(1), pp. 131-143, 2013.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters *Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data.* Proc. 13th ACM Conf. Computer and Comm. Security (CCS 06), pp. 89-98, 2006.

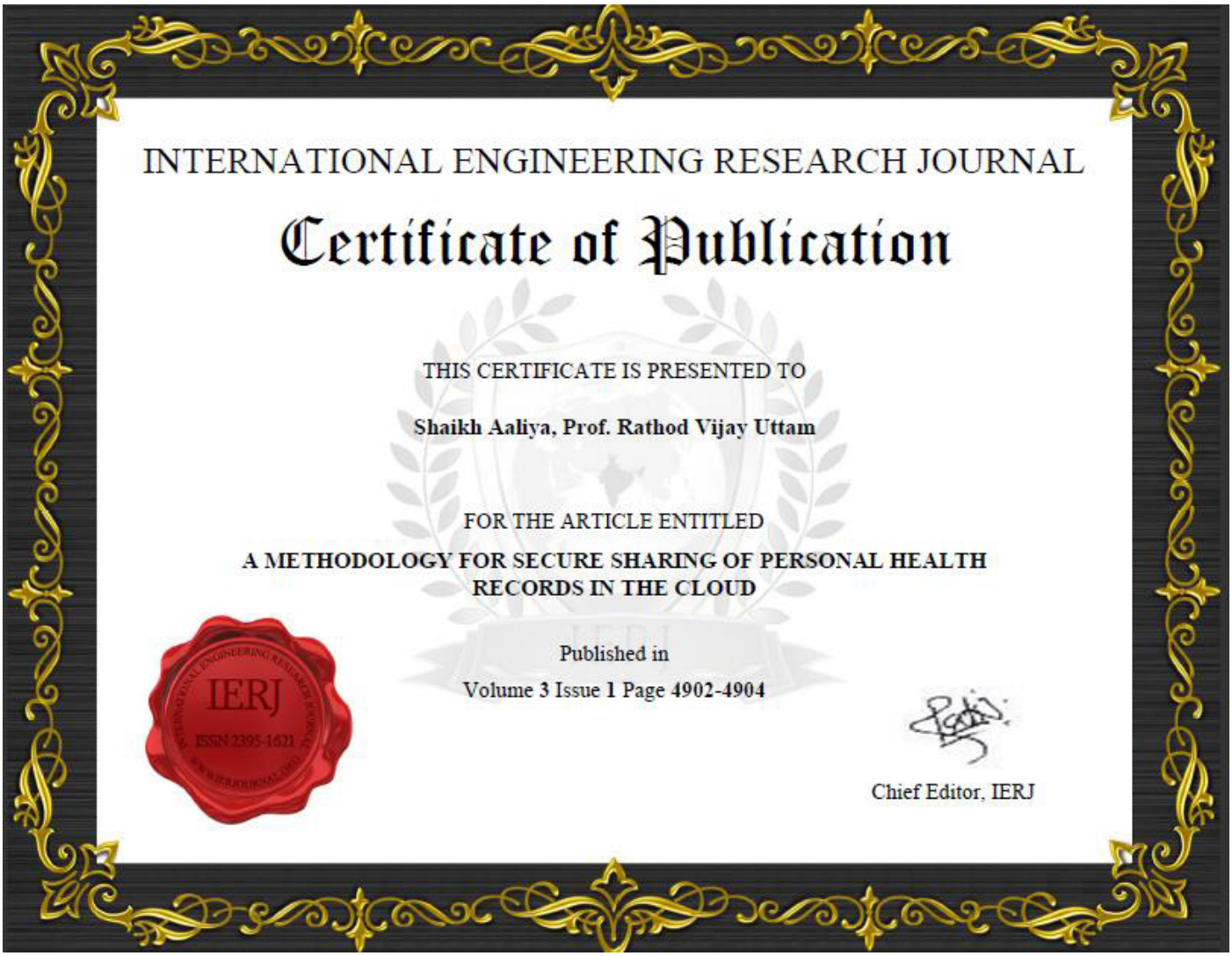
[12] M. Chase, and S.S.M. Chow *Improving Privacy and Security in Multi- Authority Attribute-Based Encryption.*in Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009

[13] R. Canetti, and S. Hohenberger *Chosen-Ciphertext Secure Proxy Re- Encryption.* in Proc. 14th ACM Conf. Computer and Comm. Security (CCS 07), pp. 185-194, 2007.

[14] M. Jafari, R. S. Naini, and N. P. Sheppard *A rights manage-ment approach to protection of privacy in a cloud of electronic health records.* in 11th annual ACM workshop on Digital rights management, October 2011, pp. 23-30.

[15] Chen Danwei, Chen Linling, Fan Xiaowei, He Liwen, Pan Su, and Hu Ruoxiang *Securing Patient-Centric Personal Health Records Sharing System in Cloud Computing,.* in China Communications, Supplement No.1, 2014

CERTIFICATES



INTERNATIONAL ENGINEERING RESEARCH JOURNAL

Certificate of Publication

THIS CERTIFICATE IS PRESENTED TO

Shaikh Aaliya, Prof. Rathod Vijay Uttam

FOR THE ARTICLE ENTITLED

A METHODOLOGY FOR SECURE SHARING OF PERSONAL HEALTH RECORDS IN THE CLOUD

IERJ
ISSN 2395-1621

Published in

Volume 3 Issue 1 Page 4902-4904

Chief Editor, IERJ

Sinhgad Institutes

Celebrating 25 Years

Sinhgad Technical Education Society's

Sinhgad Institute of Technology, Lonavala

Department of Computer Engineering

in association with

Board of Studies - Computer Engineering, Savitribai Phule Pune University, Pune

cPGCON 2018

" 7th Post Graduate Conference of Computer Engineering "

Certificate of Appreciation

This is to certify that Mr./ Ms. Shaikh Aaliya Zulfiqar

has attended the 7th Post Graduate Conference of Computer Engineering (cPGCON 2018) held on 5th - 6th April, 2018 at Department of Computer Engineering, Sinhgad Institute of Technology, Lonavala.

Ms. B. L. Dhote
Co-ordinator, cPGCON 2018
PG Co-ordinator, SIT Lonavala

Dr. S. D. Babar
Convener, cPGCON 2018
HOD, SIT Lonavala

Dr. V. H. Patil
Co-ordinator, BOS
Comp Engg, SPPU Pune

Dr. M. S. Gaikwad
Principal
SIT Lonavala

JETIR

Journal of Emerging Technologies and Innovative Research

An International Open Access Journal

www.jetir.org | editor@jetir.org

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

M/s Aaliya Shaikh

In recognition of the publication of the paper entitled

The Privacy Based Secure Sharing Of Personal Health Records a Method in the Cloud

Published In JETIR (www.JETIR.org) ISSN UGC Approved & 5.87 Impact Factor

Published in Volume 6 Issue 5 , May-2019

EDITOR

EDITOR IN CHIEF

ISSN 2349-5162

JETIR1905E19 | Research Paper Weblink http://www.jetir.org/view?paper=JETIR1905E19 | Registration ID : 211018

pgcon.png

cPGCON 2019

DPU

Dr. D.Y. Patil Unitech Society's

Savitribai Phule Pune University

Dr. D. Y. Patil Institute of Technology, Pimpri, Pune - 18

Department of Computer Engineering

cPGCON - 2019

8th Post Graduate Conference of Computer Engineering

In association with

Board of Studies, Computer Engineering, Savitribai Phule Pune University, Pune

Certificate of Participation

This is to certify that Mr./Ms./Mrs. Aaliya Shaikh has presented a paper titled as The Privacy Based Secure Sharing of Personal Health Records- a method in the cloud in the 8th Post Graduate Conference of Computer Engineering (cPGCON - 2019) held on 3rd - 4th April 2019 at Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology, Pimpri, Pune - 411018.

Prof. Rajesh Bharati
Co-Convener,
cPGCON - 2019

Dr. Pramod D. Patil
Convener, cPGCON - 2019
Vice Principal & HOD

Dr. Varsha H. Patil
Chairman, BOS
Comp Engg, SPPU, Pune

Dr. Suresh N. Mali
Principal