PERSONAL HEALTH RECORD SYSTEM BASED ON DISTRIBUTED COMPUTING

Shanthi T[1], John Augustine P[2], Amsaveni P[3]

[1]P.G Scholar, Department of CSE, Sri Eshwar College of Engineering, Coimbatore, Tamilnadu, India
[2]Assistant Professor, Department of CSE, Sri Eshwar College of Engineering, Coimbatore, Tamilnadu, India
[3]Software Engineer, FSS, Chennai, Tamilnadu, India.

Abstract- **Cloud computing system becomes more popular which allows users to access and extract the sensitive information whenever they require. This is mainly applicable in medical field, where the patients personal health information is often outsourced to be stored at a third party server, such as cloud providers. When the personal health information are stored and accessed through the proxy server, security becomes the main concerns. The main goal of this system is to protect patient's health information data confidentiality and then only the external entities such as doctors and nurses can gain access to the patient's data with the patient's consent. Hospitals are now benefitting from data sharing as this provides better, safe care of patients. There is no need to repeat medical history every time a new health professional is consulted which means no more unnecessary tests. The proposed scheme comes out with a novel encryption approach whereas the details of the patient's health information are encrypted and that encrypted text are stored in cloud database which shows security.**

Index Terms- **Personal Health Record, encryption, proxy server, cloud provider.**

I. INTRODUCTION

1. CLOUD COMPUTING

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a metered service over a network (typically the Internet).Cloud computing provides computation, software, data access, and storage resources without requiring cloud users to know the location and other details of the computing infrastructure. End users access cloud based applications through a web browser or a light weight desktop or mobile app while the business software and data are stored on servers at a remote location. Cloud application providers strive to give the same or better service and performance as if the software programs were installed locally on end-user computers.
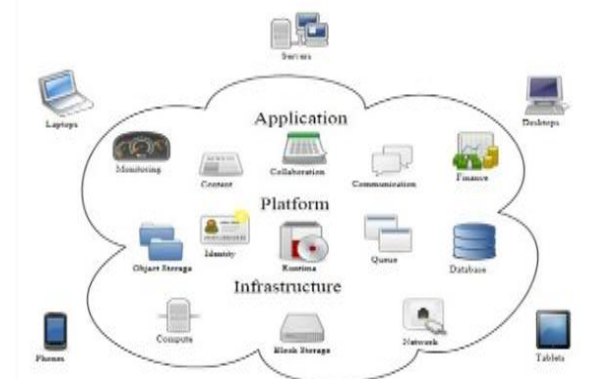

Fig 1.1 Cloud Architecture

To protect the PHR data we used attribute base encryption (ABE). Attribute is very important in attribute based encryption scheme. Attribute based encryption build the access policy using the user's private key and describe the encrypted data with the users attributes. Attribute based encryption as the two main advantages:

a. Communication overhead of the web is removed.
b. To provide the fine grained access control.

In recently years cloud has emerge to provide the many application based services satisfy the users requirements. Cloud provides the storage application in which the users are able to store the data on cloud and share it. And user can access this stored data from anywhere. We just have to pay money for required space on cloud. Cloud server is operated by the commercial provider. Storing the users data secure from storage server is not only option but it is the main

requirement of the cloud user. There are three types of cloud computing services

      1) Software as a service (SaaS)
      2) Platform as a service (PaaS)
      3) Infrastructure as a service (Iaas)

We are using cloud for personal health record data storage only in our system.

2. Attribute-based Encryption Scheme[5]

According to these schemes, a summary of the criteria, that ideal attribute-based encryption schemes, are listed as follows,

1. Data confidentiality

Before uploading data to the cloud, the data was encrypted by the data owner. Therefore, unauthorized parties including the cloud cannot know the information about the encrypted data.

2. Fine-grained access control

In the same group, the system granted the different access right to individual user. Users are on the same group, but each user can be granted the different access right to access data. Even for users in the same group, their access rights are not the same.

3. Scalability

When the authorized users increase, the system can work efficiently. So the number of authorized users cannot affect the performance of the system. *Multidisciplinary Journal of Research in Engineering and Technology,*

4. User accountability

If the authorized user is dishonest, he would share his attribute private key with the other unauthorized user. It causes the problem that the illegal key would share among unauthorized users.

5. User revocation

If the user quits the system, the scheme can revoke his access right from the system directly. The revocable user cannot access any stored data, because his access right was revoked.

6. Collusion resistant

Users cannot combine their attributes to decipher the Encrypted data. Since each attribute is related to the polynomial or the random number, different users cannot collude each other

II. LITERATURE SURVEY

M. Vijayapriya* and Dr. A. Malathi in their paper does the work related to improve the scalability. Here one to many encryption methods can be used such as ABE[5].There exits a central server where owners place their own sensitive medical data, and attempted by the users to gain access.PHR documents can be accessed by users by the server in order to read or write to someone others PHR, a user can have simultaneously have an Access to multiple owners data which needs Multi-Authority Based Encryption(MA-ABE).To provide efficient key management secure access of PHR in a patient centric manner is the main goal of this system. Vishnu Dahatonde, Ashish Jadhao, Akash Bhardwaj, Namish Diwate, Aaradhana Deshmukh One can maintain his PHR from his childhood and can use it anytime using Emergency Medical System (EMS) services which can be provided in various emergency situations. These services may include calling an Ambulance service till patient gets discharge from hospital. They develop a system that maintains PHR and provide EMS using cloud environment. It provides asynchronous notification using Google Cloud Messing(GCM)which is a lightweight mechanism that uses push messaging technology for notification.[6]

S Vidya K Vani D KavinVidya describes the framework which provides efficient key management secure access of PHR in a patient centric manner is the main goal of this system.

The user data must consist of those users who make a access based on their professional such as medical researchers, nurses, doctors role.[3]

Chang-Ji Wang1,2, Xi-Lei Xu1,2, Dong-Yuan Shi1,2, Wen-Long Lin1,2 in this paper, propose a patient centric cloud based secure PHR system, which allows patients to securely store their own PHR data on semi-trusted cloud service providers & share selectively their PHR data with large number of users, including health care provider like nurses ,doctors, family members or friends. To reduce the key management complexity for users and owners, they divide the users on cloud based PHR system into two security domains which are public and personal domain. Unlike from previous cloud based PHR system, PHR owners can encrypt their PHR data for public domain using the cipher text policy attribute-based encryption scheme. Only authorized users who satisfy the specified cipher text policy or who identifies dedicated identities can be decrypt the encrypted PHR data.

Soumya Parvatikar, Puja Prakash, Richa Prakash, Pragati Dhawale, S.B. Jadhav's proposed in

this paper that to work in attribute based encryption and cryptographically enforced the access control for outsourced data. To improve upon the scalability of the above solution is to use one-to-many encryption method such as ABE [4].

Clementine Gritti1_, Willy Susilo1, Thomas Plantard1, Kaitai Liang2 Wong3 promotes the issue of empowering patients using their health records has been well accepted in the community which is known as the personal health record i.e. PHR. We aim to provide the patients with the power of the cloud to conduct the outsourced work more efficiently. [5]

III. OBJECTIVE

The main goal of the project is to provide secure sharing of personal health records in cloud. Hospitals are now benefitting from data sharing as this provides better, safe care of patients. There is no need to repeat medical history every time a new health professional is consulted which means no more unnecessary tests. The proposed scheme comes out with a novel encryption approach whereas the details of the patient's health information are encrypted and that encrypted text are stored in cloud database which shows security.
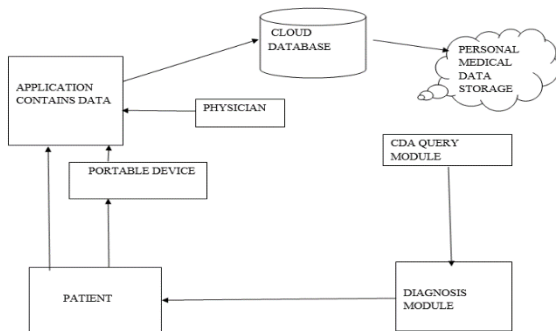
IV.ARCHITECTURE DIAGRAM

Fig. 5.1 Architecture of Personal Health Record System

V. MODULES USED

5.1 PATIENT PROFILE CREATION

A patient profile (user profile, or simply profile when used in-context) is a collection of personal data associated to a specific user[6]. A profile can be used to store the description of the characteristics of person. The user personal data store in PHR database that details contain informs like name, username, password, email Id, dob and mobile number etc.

5.2 DOCTOR PROFILE CREATION

Doctor profile is a visual display of personal data associated with a secure data[6]. A profile can be used to store the characteristics of the concern doctor. This consists of the following details namely name, dob, address, specialist and experience etc.

5.3 ADMIN MODULE

This module is used to control all the process, Admin is a super user who creates the PHR[4] data owner user and maintains the cloud server's configuration. Admin has the rights to add, edit or delete any type of data owners.

5.4 PATIENT PAGE MODULE

A patient page consists of test information, pharmacy, token booking, lab test and bill payment etc. By using his/her login id they view their particular page for their future reference. Doctor will upload the test report of an patient in this page.

5.5 DOCTOR PAGE MODULE

In the doctor page module, the doctor can upload the patients particular success stories and they can view patient details, tests etc. By using pharmacy page, the doctor can write the prescription to the patient online.

5.6 NURSE ROLE

The nurse will have the authentication to view the token bookings. After viewing it, the nurse will confirm or reject the tokens. After getting confirmation, from the nurse only, the patient can meet the doctor.

VI. IMPLEMENTATION RESULTS

6.1 HOME PAGE

Fig 6.1 shows the home page. In home page it consists of Registration for new users, login for existing users, the details of the organization and its contact details.
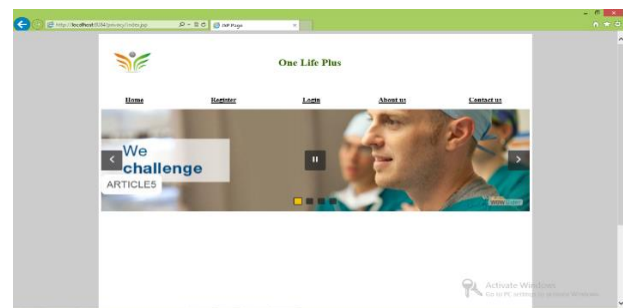

Fig 6.1 Home Page

6.2 PATIENT REGISTRATION FORM

Fig 6.2 shows the patient registration form. In patient registration page it consists of Registration for new patients with full biodata.

Fig 6.2 Patient Registration Form

6.3 ADMIN LOGIN PAGE

Fig 6.3 shows the admin login page. In admin login page it consists of login for existing users, by using correct username and password the admin can able to logon into the system.
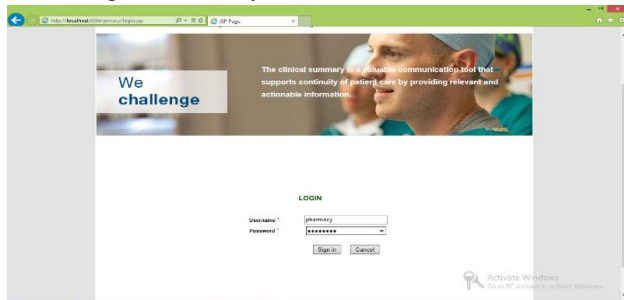

Fig 6.3 Admin Login Page

6.4 PATIENT DETAILS LIST

Fig 6.4 shows the patient details list. In patient details list page it consists of Registration for new users and login for existing users.

Fig 6.4 Patient Details List

6.5 DOCTOR REGISTRATION FORM

Fig 6.5 shows the doctor registration form page. In doctor registration page it consists of Registration for new physician with full biodata.

Fig 6.5 Doctor Registration Form

6.6 TOKEN BOOKING PAGE

Fig 6.6 shows the token booking page. In token booking page, the patient can book token for their appointment with consulting doctor.
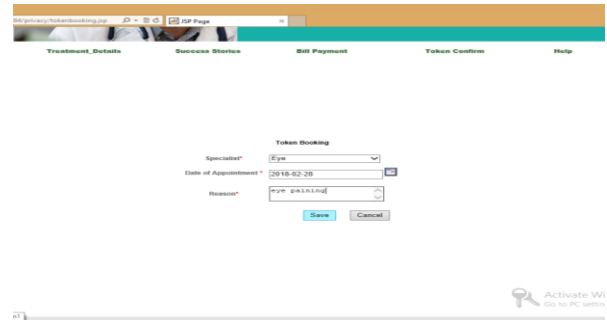

Fig 6.6 Token Booking Page

6.7 PHARMACY PAGE

Fig 6.7 shows the pharmacy page. In pharmacy page, the doctor can choose the prescribed medicine to their patient. By using this the patient can buy their medicines properly.

Fig 6.7 Pharmacy Page

VII. CONCLUSION

Cloud computing is changing our lives in many ways at a very quick space. Day by day utilization of cloud computing technologies is increasing in every part of the world. The cloud computing solutions in healthcare can help the physicians to stay in touch with their patients and examine their health condition effectively at a low cost. The attribute based encryptions and its related techniques are applied in order to enforce for the security purpose and also it will be helpful in minimizing the key management problems and complexity. For future work, the hosting can be done in order to secure the data.

REFERENCES

1. Dr.P.S.Jagadeesh Kumar and Ms.A.S.Chaithra,"A Survey on Cloud Computing based Health Care for Diabetes: Analysis and Diagnosis," in Proc. of IOSR Journal of Computer Engineering,2015.
2. Dr.S.S.Lomte and Ms. Jyoti Madhukar Shinde,"Physical Health Record System of a Patient using Cloud Computing", in Proc. of International Journal of Advance Scientific Research and Engineering Trends,2016.
3. Murugalakshmi.K, Mrs.G.Geetha and Mrs.K.Sundara Velrani,"Cloud based healthcare monitoring system using wearable sensors," in Proc. of International Journal of Emerging Technology in Computer Science & Electronics,2016.
4. R.NandhaKumar and Antony Selvadoss Thanamani,"A Survey on E-Health Care for Diabetes using Cloud Framework," in Proc. Of International Journal of Advanced Reasearch Trends in Engineering and Technology,2017.
5. Nidhi Jaini and Archana Jadhav,"A Survey paper on CDA generation and integration for Health Information Exchange based on Cloud Computing System,in Proc. Of International Journal of Innovative Research in Computer and Communication Engineering,2016.
6. Sushma S.A and Priyadarshini D.Kalewad,"Survey on Cloud Computing in Healthcare Systems," in Proc. Of International Journal of Engineering and Computer Science,2014.