International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Patient Health Record (PHR) In Cloud Security

Manikandan R, R. Karthiyayini
Department of Computer Applications, Anna University, BIT Campus, Tiruchirappalli, Tamil Nadu, India

ABSTRACT

Our project Hospital Management system includes patient's health record (PHR), storing their details into the system. Patient's health record security purpose when using RSA algorithm. It collect details record stored in cloud. It every patient's health record encrypted stored in cloud. It every patient's health record retrieve decrypted algorithm using cloud.   User can search availability of a doctor and the details of a patient using the id.The Hospital Management System can be entered using a user name and password. It is accessible either by an administrator.

Keywords : Patient's health record, RSA algorithm, Encryption and Decryption data, cloud.

I. INTRODUCTION

In most developing countries, provision of basic preventive, promotive and curative services is a major concern of the Government. With growing population and advancement in the medical technology and increasing expectation of the People especially for quality curative care, it has now become imperative to provide quality health care services through the established institutions. In public Sector 15,393 allopathic hospitals (Health Information of India 2003) are functioning. In the rural areas, the secondary level care is being provided through 3222 CHCs (Bulletin on Rural Health Statistics in India 2005) with 30 beds each with specialist services of physicians, pediatricians, O & G specialists, and surgeons being made available. However, these services have not been successful in gaining the faith and Confidence of the people because of lack of specialists, facilities and accountability, along with the paucity of resources and non-involvement of the community.

II. LITERATURE SURVEY

This paper is mostly related to works based on security of PHR in cloud computing in which most of them are based on Attribute Based Encryption techniques. Ming Li and Shushing Yu did research on sharing personal health records using attribute based encryptions and tried to achieve a fine– grained and scalable data access control for PHRs They guarantee a high degree of patient privacy simultaneously by exploiting multi-authority ABE. This scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios [1]... Pooja K. Patel and P. M. Pawar also performed the encryption of PHR for enhancing the security of the data using Attribute Based Encryption in Cloud Computing. The paper discusses the use of cloud computing and cryptographic techniques i.e. (ABE) for Personal health record (PHR) as PHR is an upcoming patient-centric model for storing patient's e-record in one centralized place. It allows patients to create, manage, control and share their health information with other users as well as health care providers. [2]. Another work related to this was done by Jitendra Madarkar, Anuradha D and Sachendra Waghmare who discussed about achieving the security of PHR by using the RSA Algorithm and also Attribute Based Encryption and finally storing the data in the Cloud Environment. According to this work, E-hospital record user can access and store health record like emergency information like blood group, medication history and electronic prescription. In cloud E-hospital record store and process very sensitive patient data and should have a proper privacy framework and security mechanism since the reveal of health record may have social result consequence especially for patients [3]. Able E Alias and Neethu Roy worked on improving security of Attribute Based Encryption for secure sharing of personal health records. This paper proposes that to ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi trusted servers. For this reason they propose a new system that ensures the security of PHR

III. EXISTING SYSTEM

This approaches may occur problems because the patient missed their reports. This types of reports are hard to store in many years. iii. Till now, most hospitals are not have an each patient prescriptions, x- ray, scan reports etc.

IV. PROPOSED SYSTEM

Modules in Hospital Management System:

The most important concern of a HMS is the efficient patient management, which is a significant challenge. Everything today depends on technology and here we are implementing an electronically managed health record called PHR which manages the health details of each patient online. In order to maintain this PHR of every patient online, the Hospital Management System needs to be categorized into various modules which are as follows:

Admin Module:

It is the first and most important domain of any management system i.e. they are the ones who controls everything. But here the admin module is the one who controls registration and removal of various hospitals in the HMS. The services of hospitals which are registered can be. Accessed by the registered patients. Admin is the one who provides approval to patient acceptance.

Patient Module:

It is the main or most important module in our HMS. Patient module provides the control of their own PHR to each patient. He can decide who all can access the PHR. A patient can register into the HMS and when accepted by admin will become a member of the system. He can avail services from each and every hospitals that are registered in the system. So here in this system the patient who may approach various hospitals at various different places need not carry their medical reports by hand as everything will be stored online in a very secure manner. The main feature of this i.e. the security is been given priority and as a result of which the PHR of different patients are stored after encrypting it with RSA Algorithm into a cloud environment from where the hospitals and doctors registered in the system can access it when patient goes for checkups.

Doctor Module:

In this module, the doctors are included who will be registered by the hospital module which also have the rights to remove a doctor from the system if required. The new doctor add, update, delete from this module. In this module doctor to will be check in PHR files in your patient report.

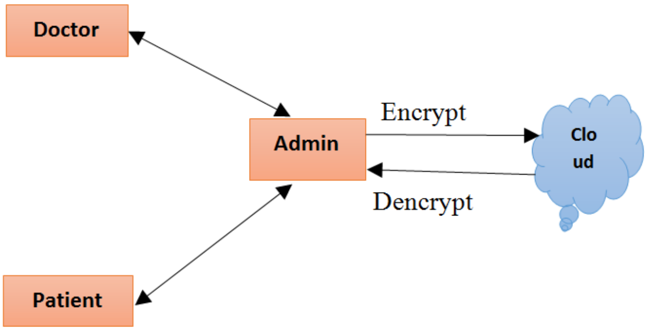


Figure 1. The architecture of the proposed system

V. SYSTEM SPECIFICATION

Hardware specification:

SYSTEM: Pentium IV2.4 GHz
HARD DISK: 40GB
MONITOR: 15VGA Color
RAM: 1GB
KEYBOARD: 110 keys enhanced

Software specification:

OPERATING SYSTEM: Windows XP and above
FRONT END: R Tool
BACK END: Excel

RSA Algorithm:

This algorithm is based on the difficulty of factorizing large prime numbers i.e. the numbers that have only 2 factors. Here the system works on the basis of a public and private key system where the private key is made secret. The public key will be made available to everyone as it is not a secret key. Using this key a user will be able to encrypt data but will not be able to decrypt it, the one who will be able decrypt it is the one who possesses the private key. Even though theoretically possible, it is extremely difficult to generate the private key from the public key, which makes the RSA algorithm a very popular choice in data encryption.

Step 1: Assume two large prime numbers p & q

Step 2: Compute: N = p*q where N is the factor of two large prime number.

Step 3: Select an Encryption key (E) such that it is not a factor of (p-1)*(q-1).i.e. Ø (n) = (p-1)*(q-1) for calculating encryption exponents E, should be 1< E < Ø (n) such that gcd (E, Ø (n) =1.Here we are calculating gcd because E & Ø (n) should be relative prime. Ø (n) is the Euler Totient Function & E is the Encryption Key.

Step 4: Select the Decryption key (D), which satisfy the Equation D*E mod (p-1)*(q-1) = 1

Step 5: In case of Encryption: Cipher Text= (Plain Text) E mod N CT = (PT) E mod N or CT=ME mod N

Step 6: For Decryption: Plain Text= (Cipher Text) E mod N PT= (CT) E mod N

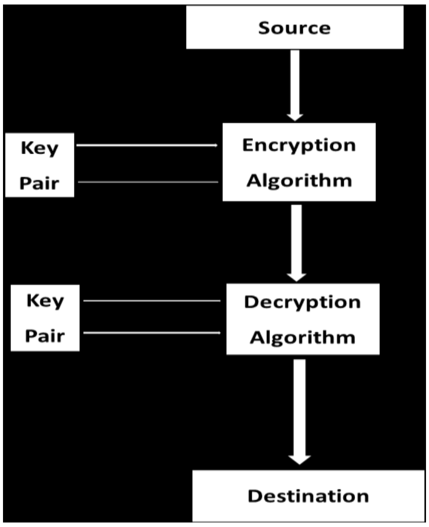
Encryption algorithm:

Step 1. Function or key generation is the step of generation of two keys called public key and private key.

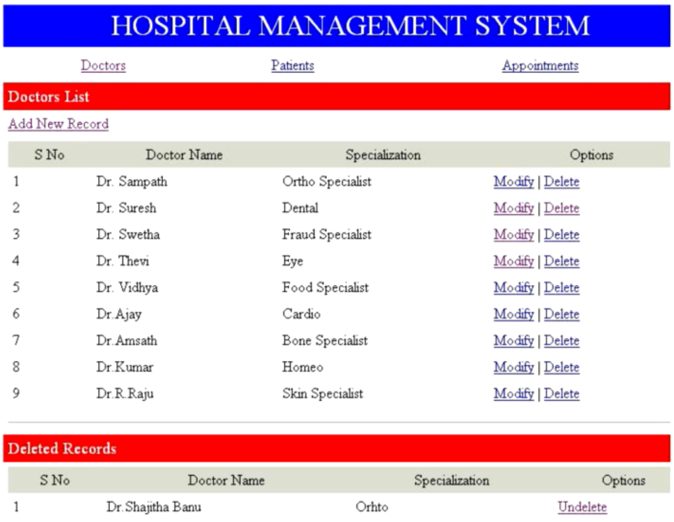
Step 2. Encryption: plaintext P encrypted using public key to generate cipher text C.

Step 3. Decryption: Cipher text decrypted by private key to retrieve the plain text P.

Step 4. Evolution: output a cipher text C off (p).



VI. RESULTS



HOSPITAL MANAGEMENT SYSTEM

Doctors Patients Appointments

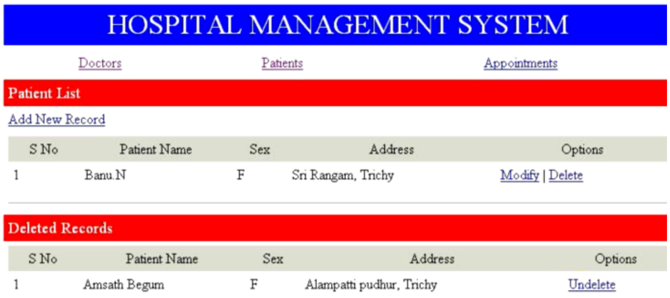
Doctors List

Add New Record

S No	Doctor Name	Specialization	Options
1	Dr. Sampath	Ortho Specialist	Modify | Delete
2	Dr. Suresh	Dental	Modify | Delete
3	Dr. Swetha	Fraud Specialist	Modify | Delete
4	Dr. Thevi	Eye	Modify | Delete
5	Dr. Vidhya	Food Specialist	Modify | Delete
6	Dr.Ajay	Cardio	Modify | Delete
7	Dr.Amsath	Bone Specialist	Modify | Delete
8	Dr.Kumar	Homeo	Modify | Delete
9	Dr.R.Raju	Skin Specialist	Modify | Delete

Deleted Records

S No	Doctor Name	Specialization	Options
1	Dr.Shajitha Banu	Orhto	Undelete



HOSPITAL MANAGEMENT SYSTEM

Doctors Patients Appointments

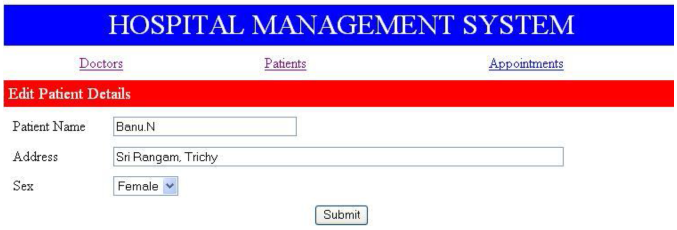
Patient List

Add New Record

S No	Patient Name	Sex	Address	Options
1	Banu.N	F	Sri Rangam, Trichy	Modify | Delete

Deleted Records

S No	Patient Name	Sex	Address	Options
1	Amsath Begum	F	Alampatti pudhur, Trichy	Undelete

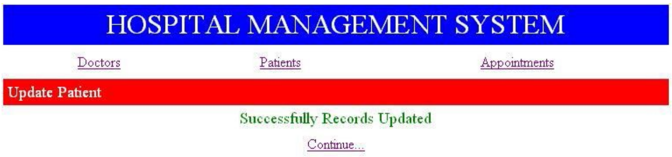


HOSPITAL MANAGEMENT SYSTEM

Doctors Patients Appointments

Edit Patient Details

Patient Name	Banu.N
Address	Sri Rangam, Trichy
Sex	Female



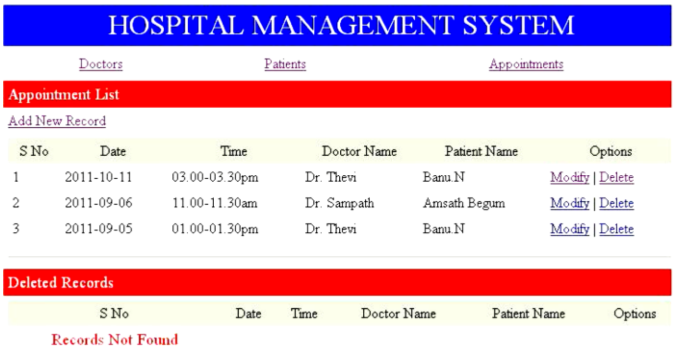
HOSPITAL MANAGEMENT SYSTEM

Doctors Patients Appointments

Update Patient

Successfully Records Updated

Continue...



HOSPITAL MANAGEMENT SYSTEM

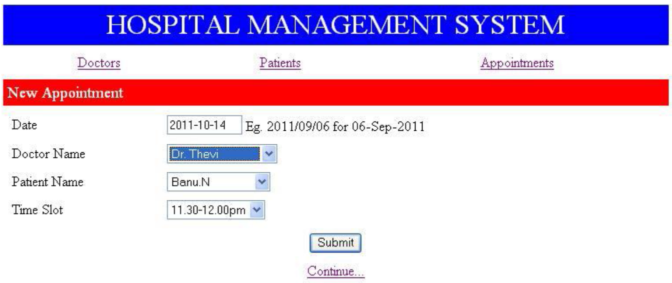
Appointment List

S No	Date	Time	Doctor Name	Patient Name	Options
1	2011-10-11	03.00-03.30pm	Dr. Thevi	Banu.N	Modify | Delete
2	2011-09-06	11.00-11.30am	Dr. Sampath	Amsath Begum	Modify | Delete
3	2011-09-05	01.00-01.30pm	Dr. Thevi	Banu.N	Modify | Delete

Deleted Records

S No	Date	Time	Doctor Name	Patient Name	Options

Records Not Found



HOSPITAL MANAGEMENT SYSTEM

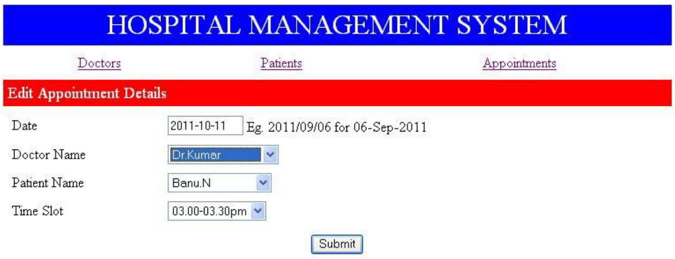
New Appointment

Date 2011-10-14 Eg. 2011/09/06 for 06-Sep-2011

Doctor Name Dr. Thevi

Patient Name Banu.N

Time Slot 11.30-12.00pm



HOSPITAL MANAGEMENT SYSTEM

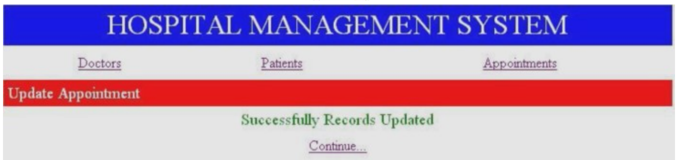
Edit Appointment Details

Date 2011-10-11 Eg. 2011/09/06 for 06-Sep-2011

Doctor Name Dr.Kumar

Patient Name Banu.N

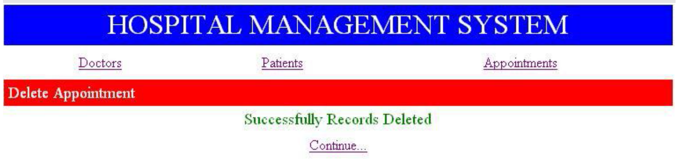
Time Slot 03.00-03.30pm



HOSPITAL MANAGEMENT SYSTEM

Update Appointment

Successfully Records Updated



HOSPITAL MANAGEMENT SYSTEM

Delete Appointment

Successfully Records Deleted

VII. CONCLUSION

In this paper, a detail design of implementation of HMS for secure sharing of personal health records in Cloud Computing is performed. After considering the fact that cloud servers are partially trust worthy, in order to ensure security of PHR we are encrypting the data before we store it into the cloud environment. And also a patient-centric concept is used as a result of which patient has the complete control of their own privacy and a fine grained access is obtained. Here the use of different modules like admin, patient, doctor works in coordination and forms a complete and efficient HMS. And also the unique challenges brought by multiple PHR owners and users are addressed in that the complexity of key management is reduced when number of owners and users in the system is large.

VIII. REFERENCES

[1]. CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD Monjur Ahmed and Mohammad Ashraf Hossain

[2]. Cloud Computing Research and Security Issues. Jianfeng Yang, Zhibin Chen

[3]. Cloud Computing Security Issues in Infrastructure as a Service, Pankaj Arora* Rubal Chaudhry Wadhawan Er. Satinder Pal Ahuja

[4]. Security and Privacy in Cloud Computing: A Survey Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou.

[5]. Study of Security Issues in Cloud Computing Varsha