Enhancing Security of Personal Health Records in Cloud Computing by Encryption

Nishitha Ramakrishnan[1], **Sreerekha B**[2]

[1] PG Student (M.Tech, CSE), Malabar Institute of Technology, Anjarakandy (P.O), Kannur, Kerala, India

[2]Associate Professor, Department of CSE, Malabar Institute of Technology, Anjarakandy (P.O), Kannur, Kerala, India

Abstract*: Efficient Management of Hospital data and correct maintenance of Patient Health Record (PHR)'s is a significant challenge. With online PHR, patient can manage their own medical records in an efficient way. The most important thing to be considered in this is the security of data which can be done efficiently by storing PHR's using Cloud Computing. Even though cloud data storage provides an important aspect of quality of service in terms of security in this paper PHR's are encrypted using RSA Algorithm before it is been stored to the cloud environment. In this paper, the Hospital Management System (HMS) is divided into four modules which include admin, patient, hospital and doctor modules all of which acts in coordination for proper working of Hospital Management System. In order to achieve scalable and secure data access controls of the PHR's the complete control of the PHR is given to that patient itself. In this system, the users who all can access the PHR's are divided into multiple security domains like the Health Care domain, the public domain which greatly reduces key management complexity for the patient and users of PHR. The advantage of the methodology used is that even real time service from doctors can be obtained for patient by referring the PHR of the patient online.*

Keywords: Personal Health Record, Hospital Management System, Cloud Computing, RSA Algorithm, Health Care Domain

1. Introduction

Health Care is one of the major challenges that India is facing today. The usage of technology in the field of health care is at a minimum. A doctor needs to know the complete history of the patient before he could make a proper diagnosis, but this information is difficult to be maintained as each patient may consult a no of doctors during his lifetime. Most people receive health care from more than one doctor-a family physician dermatologist, an orthopedist or a cardiologist. The records each physician gathers on your health and treatment details are scattered across offices all over. Informing each doctor of all the conditions tests, and treatments is difficult during an appointment and sometimes you may not know what information is important. Not having access to your complete medical record has consequences which can be potentially life threatening. Tests may be unnecessarily repeated, wasting time and money. Symptoms may be over looked which may lead to an incorrect treatment. There may be cases when dangerous combinations of medications may be accidentally prescribed which may cause serious health problems. Healthcare is a field in which accurate record keeping and communication are critical and yet in which the use of computing and networking technology lags behind when we compare it with other different fields. The professionals in Healthcare and the patients are often uncomfortable with computers and latest technologies, and feel that computers are not very necessary to their healthcare environment, even though the healthcare professionals agree that accurate record keeping and communication are essential for effective hospital management. In the current healthcare system, information is conveyed from one healthcare professional to another through paper notes or personal communication and errors in which may cause serious health problems to people where even chances of death exists.

E-Care provide a platform where patient's medical records are stored and readily accessible by any doctor who the patient visits. This platform helps the patient maintain a Patient Health Record (PHR) which is highly a patient-centric model for effective storing of health data. The E-Care system not only stores the patient's medical records but also uses the data to provide real time information. Using this data, there is also a facility of patients posting queries to doctors all over the world and getting treatment without physically meeting him. In order to ensure the security of the PHR's, we are storing it using Cloud Computing after encrypting it with RSA Algorithm. The biggest advantage of storing PHR in cloud computing is that users can access data stored in the cloud anytime and anywhere using any device in a secure manner [2]. The PHR owner, which is the patient himself decides how the records need to be encrypted and to which all users the keys must be shared. In addition to this, the patient has the full rights to stop any user from accessing his PHR whenever required. The management of keys a is a critical task as there includes generation of public and private keys in RSA Algorithm and the task of efficient management of the private keys follows.

Whenever a person feels sick or suffers from any kind of disease, he visits a doctor who prescribes him certain medicines taking of which he might have got cured. Later on when he again falls sick he might be at a different place and may go for treatment at some other doctor who may ask the patient for the previous prescription or medicines taken earlier or if any allergy conditions occur for the patient by taking any of the medicines. But for the patient it is difficult to carry the medical records and files all the way he travels. In this paper, there is exact solution for this particular problem i.e. efficient management of PHR using Cloud Computing that too only after encrypting with RSA Algorithm that can be retrieved online any time any place.

The idea behind this approach is that the PHR can be shared among two kinds of domain in two different ways:

1) Open Access Domains: The open access domains are those which access are given openly or a direct access is been allowed in this case. The main feature of open access domains is the Health Care domains i.e. Hospitals and the HealthCare professionals. Here various hospitals can be registered in the HMS where the registered doctors in the hospitals can access the PHR's of patients coming for checkup and provide the required treatment.
2) Closed Access Domains: This is the type of domain where direct access is not possible and whoever needs to access the data of the PHR for eg. a patient's friend or relative, he may have to send the request to the concerned patient and only if the patient provides the friend with the required private key and then only he can access the datas of the patient. Here basically, only the primary or very essential details of a patient like his name, age, sex, height, weight etc. will be visible to an outsider.

2. 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 Shucheng 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. Patil 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 patients 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. That is been done using ABE Algorithm [4]. Yet another work done for improving the situation of a hospital system in order to be able to handle also the emergency patients done by implementing situation aware environment and providing an enhanced patient management was done by Philip Moore and Andrew Thomas. This paper postulates that technology enhanced patient management based on intelligent situational awareness has the capability to improve patient experience with improvements in resource utilization in a hospital setting [5].

3. Proposed System

3.1 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:

1) *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.
2) *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.
3) *Hospital Module*: It is the module which register various hospitals and doctors to the hospital management system. Using this module, either the hospitals can register to the system which will be accepted or rejected by the admin or the admin module can directly add different hospitals.
4) *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 doctor can view the PHR of the patient when a patient goes for a checkup and also can add their latest prescriptions or views to the already existing PHR.

They can also suggest for any test if required to the patient.

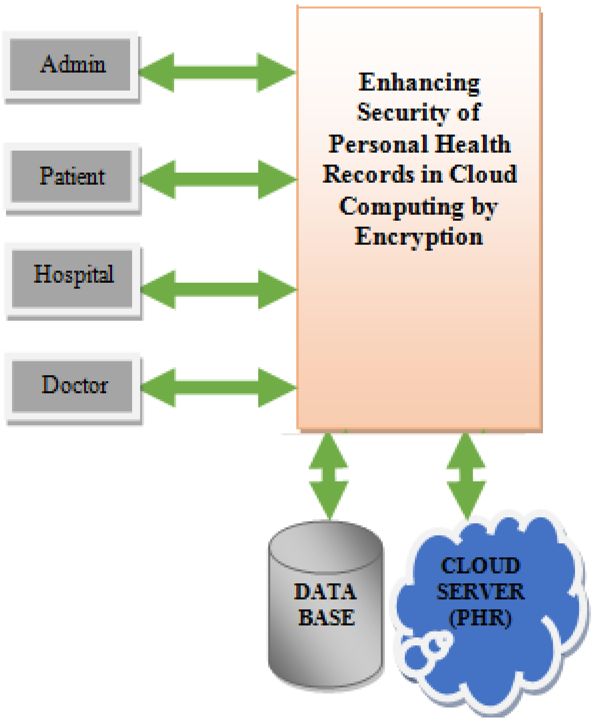
Admin
Patient
Hospital
Doctor
Enhancing Security of Personal Health Records in Cloud Computing by Encryption
DATA BASE
CLOUD SERVER (PHR)

Figure 1: Architectural Design of HMS

With the proper working and co-operation of these modules, the HMS forms an efficient system for the proper management of PHR of each patient.

3.2 Storing PHR in Cloud Environment

When PHR services are introduced for every patient, there are many risks in terms of security and privacy which could impede its wide adoption. The important concern is about whether the patients can actually control the sharing of their sensitive and private personal health information, that too when they are stored on a third-party server which are not completely trustful. It is essential to have fine-grained data access control mechanisms that work with semi trusted servers to ensure patient-centric privacy control over their own PHRs [4]. Patient Health Record include all the medical details of a particular patient i.e. the diseases he has suffered from and the treatments or cures that have been taken for various treatments. There may be cases where a patient might have suffered from cancer and taken medications and got cured completely. So that patient may not be interested to reveal these health details to all. So each and every patient wishes that their health records are stored in a secure and confidential manner. In order to ensure this security we are storing the PHR’s using Cloud Computing and only after encrypting it with the RSA Algorithm the concerned algorithm since includes two keys i.e. public and private keys, ensures a full guarantee with the case of security there after PHR is been stored in the Cloud it can be accessed only by open domains which includes the Health Care domains and the remaining users can access the data only after requesting the patient and the patient providing the private key if the user found a legal one. The greatest advantage of cloud computing is that users can access data stored in the cloud anytime and anywhere using any device, such as thin clients with minimum memory capabilities processing and bandwidth. After considering these merits of cloud computing, we are putting the idea of PHR model storage onto it which provide a secure and safe environment [2].

3.3 RSA Algorithm

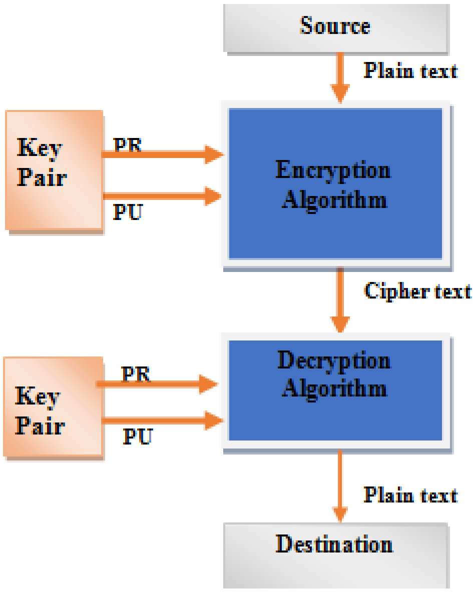

Figure 2: Implementation of RSA Algorithm

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

3.4 PHR Management using Cloud Computing

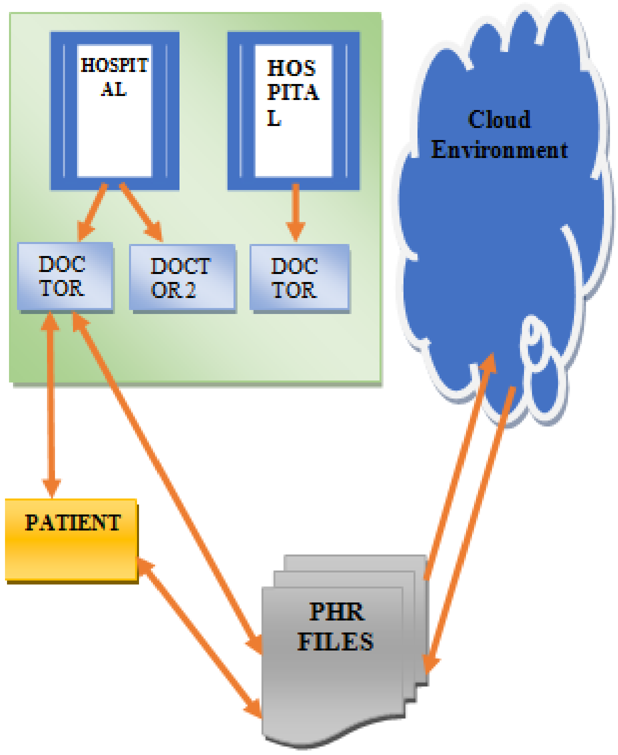

Figure 3: Management of PHR using Cloud Computing

In the given architecture of a Hospital Management System, the main entities are hospitals which are registered in the HMS, doctors registered in the various hospitals, patients coming for treatment, their PHR files and the cloud server. A patient can visit any of the hospital which are registered to the HMS and then the Hospital registers the patient into the system and also the patient can directly register to the system which will be approved by the hospital module. Now after that the patient can avail the services from the concerned doctor and the records or details of the treatment of the patient will be stored in the PHR of that patient and this PHR will be encrypted using RSA algorithm and stored in the Cloud Environment by the patient. Later on when patient gets treatment from another doctor from yet another hospital then that doctor can download the PHR of the concerned patient from the Cloud Environment and refer to the previous case history of the patient for providing better treatment to the patient.

Encryption algorithm:
1. Function or key generation is the step of generation of two keys called public key and private key.
2. Encryption: plaintext P encrypted using public key to generate cipher text C
3. Decryption: Cipher text decrypted by private key to retrieve the plain text P.
4. Evolution: output a cipher text C off (p).

One method is to allow PHR owner patient to access PHR data from cloud by selective sharing in order to avoid the risk of confidential exposure [14]. Instead of the cloud owner encrypting the health record (data), patient can generate their own decryption keys using ABE (attribute-base encryption) and then distribute them to their healthcare authorize users. Patients could a select fine-grained way which part of their patient health record by encrypting the record allowing to a set of attribute and which user can have access. Whenever the situation comes that the patient wants to reject access of other users, patient can do that. With this model a patient-centric PHR system can be created in which multiple owners can encrypt data using different sets of cryptographic keys. This approach provide flexible health record access policy that allows some changes in emergency condition within which the regular access control policies could be broken to allow a type of emergency access. However there may occur some communication overhead during key distribution and health record management or user management, which this model or approach does not address. The challenge of huge computation can be solved by using some methods by which owner performs all operation of data and user management besides re-encryption by protecting data privacy against cloud owners. This is possible when PHR owner transfer the computation task involved in fine –grained data access control to the cloud service provider without revealing the original content [3].

4. 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, hospital, 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.

References

[1] Ming Li , Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, Senior Member, IEEE "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption", IEEE

2012 Transactions on Parallel and Distributed Systems,Volume: 11 , Issue: 2.

[2] Pooja K. Patil and P. M. Pawar,” PHR Model using Cloud Computing and Attribute based Encryption”, International Journal of Computer Applications (0975 – 8887) Volume 65– No.18, March 2013.

[3] Jitendra Madarkar, Anuradha D and Sachendra Waghmare,” Security issues of Patient Health Records in E-Hospital Management in Cloud”, International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-6),June 2014.

[4] Able E Alias and Neethu Roy,” Improve Security of Attribute Based Encryption for Secure Sharing of Personal Health Records”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6315-6317.

[5] Philip Moore and Andrew Thomas, “Situational Awareness for Enhanced Patient Management” 2013 Seventh International Conference on Complex, Intelligent, and Software Intensive Systems,pp. 493-298.

[6] Ming Li1, Shucheng Yu, Kui Ren and Wenjing Lou,” Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings”.

[7] Maya Louk, Hyotaek Lim and Hoon Jae Lee,” Security System for Healthcare Data in Cloud Computing”, International Journal of Security and Its Applications Vol.8, No.3 (2014), pp. 241-248.

[8] Daniel B. Neill,” Using Artificial Intelligence to Improve Hospital Inpatient Care”, © 2013 IEEE intelligent systems Published by the IEEE Computer Society.

[9] Nidhi Kushwaha, Shashank Sahu and Rajesh Kumar Tyagi “ Evolving Intelligent Agents for Hospital Management System”,2013 3rd IEEE International Advance Computing Conference (IACC) ,pp. 902-907.

[10] Cong Wang, Qian Wang, and Kui Ren,” Ensuring Data Storage Security in Cloud Computing”.

[11] Pradnyesh Bhisikar and Amit Sahu,” Security in Data Storage and Transmission in Cloud Computing”,International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013

[12] Kevin, Murat, Latifur and Bhavani ,”Security Issues for Cloud Computing”,supported by AOFSR project on Secure Information Grid.

[13] S. Vidya, K. Vani, D. Kavin Priya,” Secured Personal Health Records Transactions Using Homomorphic Encryption In Cloud Computing”, International Journal of Engineering Research & Technology (IJERT).

[14] Ming Li1, Shucheng Yu1, Kui Ren2, and Wenjing Lou1,” Securing Personal Health Records in Cloud Computing: Patient- Centric and Fine-Grained Data Access Control in Multi-owner Settings”,, Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2010.