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

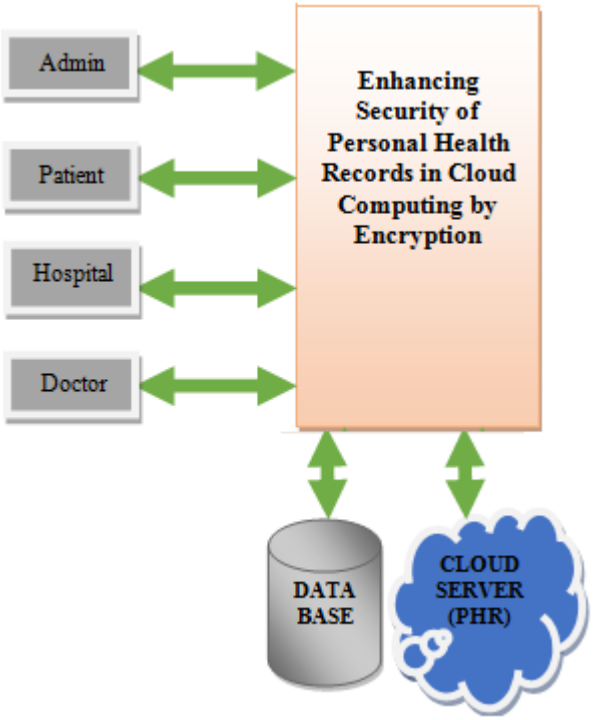

Figure 1: Architectural Design of HMS

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

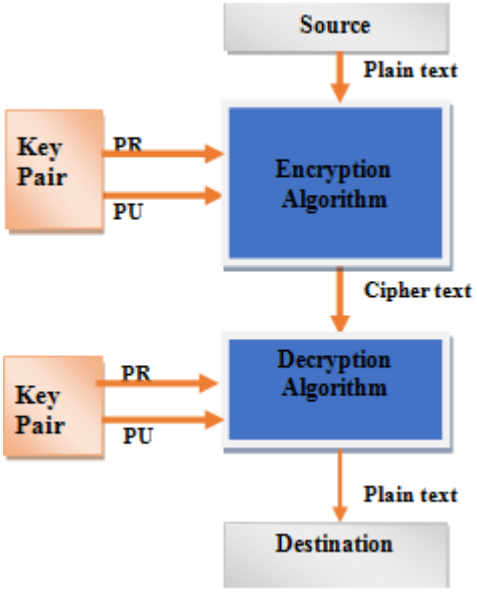

Figure 2: Implementation of RSA Algorithm

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

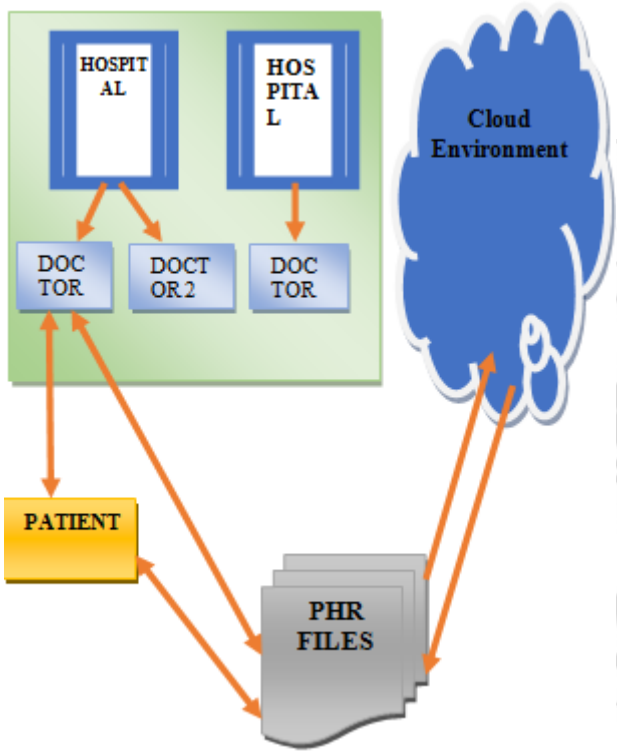

Figure 3: Management of PHR using Cloud Computing

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.