NHIS-An Approach to Privacy Preservation of Health Care Records in Cloud Computing Environment

Arjun U.
Asst.Professor
Dept.of ISE, PESITM
Shimoga, Karnataka, India

Vinay S.
Associate Professor
Dept.of CSE, PESITM
Shimoga, Karnataka, India

ABSTRACT

Cloud computing is known for its elastic and on-demand services. Cloud users can enjoy all the resources being provided by the cloud for a certain charge. Cloud users will be charged on the basis of pay-as-you-go model. Data storage is the mostly needed service nowadays. The cloud users submit their data to the cloud and remain relaxed as there will not be any problem in data maintenance. However, privacy is the major concern here. National Healthcare Info System (NHIS) has got terabytes of health care data and has to be managed effectively. Thus, the merit of cloud computing is enjoyed and the shortcomings are needed to be overcome. All the health care data is submitted to the cloud and users or patients can access it only when the One Time Password (OTP) is provided. This OTP is a 6 or 8 digit randomly generated number by RSA. Thus, privacy is ensured and also the identity of the client is provided by the modification of IP address, which is the task of intermediary layer. This proposed system comprises of three layers namely client, intermediary and privacy preservation layer.

Keywords

Cloud Computing, Health Care Records, OTP, Privacy Preservation.

1. INTRODUCTION

Cloud computing has gained its limelight because of its on-demand and elastic service. Many services are offered to the cloud users by the cloud providers by employing powerful datacenters. One of the powerful services rendered by cloud is data storage.

Cloud users can put an end to the problem of data and memory management. This makes sense that cloud users provide all their data to the cloud provider, in order to save space and cost. However, data outsourcing introduces the issue of security that the confidential or sensitive data can be misused. So, such data has to be kept private and confidential.

In order to forbid the successful implementation of cloud, a cloud provider is expected to provide a strong privacy preserving policy to the cloud users.

Cloud's service can be categorised into Software as a Service (SaaS) which is the service made available by the cloud such that the cloud users can be able to access the applications over network.

Platform as a Service (PaaS) makes sense that the cloud user can build anything with the platform (e.g. Operating System) provided by the cloud.

Infrastructure as a Service (IaaS) is a type of service in which the supporting equipments such as storage, servers, hardware and much more are provided to the cloud user for some cost. Here, the cloud follows the policy of pay-as-you-go model.

A cloud can be of four types and they are as follows. Public Cloud is the cloud that offers resources to the general public over network and the users will be charged for what they used and there is no minimal fee.

Private Cloud is the type of cloud that is meant for a single party or an organization.

Here, the users can be from a single organization.

Community cloud is the cloud that allows its infrastructure to be shared by different organizations with same focal point.

Hybrid cloud can be claimed as the combination of public, private and community clouds. In this cloud, the service provider can utilize the third party cloud service provider, aiming at increasing the flexibility.

Some of the advantages of using cloud are its inexpensiveness that is the infrastructure is not needed to be built but can be rented. Increased data storage is encouraged by cloud, which means that tera and peta bytes of data can be placed in a cloud without any struggle as the cloud is based on the principle of elasticity.

In spite of all these advantages, cloud has still got many challenges such as data security, data recovery and data management etc.,

As time grows, a systematic innovation is needed for providing a cost effective, efficient and high quality service, when healthcare is concerned. It is strongly believed that cloud can enhance the healthcare services effectively.

Many healthcare organizations started to utilize cloud so that the organizations can escape from buying own servers and software, patient record management and patient care governance.
Usually, smaller hospitals or laboratories do not have IT staffs for the management of Electronic Health Records (EHR), and hence cloud would be a boon as the smaller entities no need to afford much for data storage and initial start up cost.
When larger health organizations are concerned, the data management can be totally handled up by the cloud which is scalable and flexible. Also, cloud computing uses its resources effectively that is based upon the need of the organization, the computing resources are altered and hence cost saving is achieved.
This paper is organized as follows. Section II carries Literature Survey and section III is presented with the proposed work. Section IV deals with the process flow of the system and finally concluding remarks is presented.

2. LITERATURE SURVEY

The work proposed in [1] has provided a solution to automate the process of collecting and analyzing patient's data. This is achieved by the sensors attached with the medical equipments and the medical data is made available for the medical centre's cloud. The merit here is it removes the overhead of collecting all such data manually and also the information is made available all the time.

A cloud computing framework is proposed in [2], in which a cloud computing protocol management model that provides multimedia sensor signal processing and security is presented. Thus, the mobile devices are no longer needs to execute heavy multimedia and security algorithms in order to provide mobile health services.

The work proposed in [3] has introduced a cloud initiative named 'Dhatri' that utilized the cloud computing at the maximum coupled with wireless technologies, so as to provide physicians the data access on anywhere and anytime basis.

Personal Health Records (PHR) based Emergency Medical Systems (EMS) on the basis of cloud computing is presented in [4]. This work claims that the patient's data can be easily accessed from anywhere and thus the emergency care can easily be handled.

A medical and a health information system are proposed on the basis of cloud computing in [5]. The proposed system is claimed to be cost effective and efficient so as to share and co-ordinate medical information.

The work presented in [6] constructs a 8Hospital Information System (HIS) by employing a network module connected within the hospitals. This work follows cloud computing and thus information sharing and high end processing is made possible.

Medical image storage, exchange and sharing issues of Electronic Medical Records (EMR) are handled by the proposed Medical Image File Accessing System (MIFAS). This system increases the efficiency of information sharing between the patients and the physicians [7].

A new intelligent management system based on cloud is proposed in [8] and this work proves its efficiency in utilizing the medical records.

In [9], the concept of integration and sharing of Electronic Health Records (EHR) in healthcare clouds is discussed and also the security and privacy issues concerned with the access and management of EHR is provided.

The proposed system is composed of three layers namely client, intermediary and privacy preservation layer. The intermediary layer modifies the IP address of the client, so as to reduce the degree of identity. The privacy preservation is taken care of by the privacy preservation layer, which generates a One Time Password (OTP) by exploiting RSA and the privacy is preserved.

3. PROPOSED WORK

3.1 Overview

With the wide usage of Electronic Health Records (EHR), there is a strong requirement of creating a secure EHR model for effective sharing of data and integration. When these EHR is clubbed with cloud, the data access is much easier. However, there are several issues related to security and privacy.

Cloud provides its maximum potentiality for granting quick access to healthcare records. With cloud computing, the patient is provided provision with accessing health records from anywhere, provided the patient has got network connection.

The security issues in a cloud can range from trust, identity management, data protection and availability.

Trust is the level of reliability that an entity have on another. In fine, the more the user can control their data, the more will be their trust. The cloud service is based on Service Level Agreements (SLA) and this is to shoot up the level of trust of the cloud users. However, trust can be gained only when the SLAs are strictly followed. It is necessary to prevent failures rather than post failure compensation.

In this work, we consider most of the security breaches such as identity management, data leakage and access control. The proposed work follows a layered architecture that comprises three layers namely, Client layer, Intermediate mapping layer, Privacy preservation layer, replica management layer.

The underlying Client layer requests the server in order to gain access to the cloud services. The next layer named as intermediate mapping layer aims at altering the IP address of the client, in order to keep the degree of identity less. Also, the privacy of user's IP address is ensured.

Privacy preservation layer aims at providing privacy to the user and the data as well. This layer allocates a dedicated thread to a particular user also a One Time Password (OTP) is provided to the user in order to have increased security.

Data availability is ensured by replicating the medical data, such that the confidential data can be recovered at any instant of time. The data may be lost due to natural calamities or any unfavourable conditions. Under such circumstances, the data can be rescued without any problem as the duplication of data is present.

However, data availability has got many overheads such as updating the replicas once the parent data is modified and this is not an easy task. However, this is not the scope of our paper.

3.2 Proposed Methodology

If a person wants to be a member of National Healthcare Info System (NHIS) , the person has to enrol himself in a desired plan provides by the NHS. Initially, after having completed the check up by the physician, the patient may be directed to produce some test reports which may be of laboratorial or scanning based.

The results provided by these tests are submitted to the NHIS in order to give hands for the subscribed users. Issues hit the scene, when a large amount of data is needed to be maintained. In this scenario, all the submitted results are handed over to a cloud in order to reduce the overhead of data maintenance.

It is very essential to ensure the security of such healthcare records of every person. Thus, this work proposes a secured model for maintaining healthcare records with privacy and security.

As soon as the person enrol himself in a NHIS with an ID proof, the Trust Authority (TA) will verify the identity of the person and then the id is provided to the person, such that the person can log in to the cloud to know the test results. The test results are uploaded by the IT staff of scanning or laboratory section.

After logging to the NHIS system, the user will be provided with a One Time Password (OTP), in order to gain access to the health records. This ensures the security of the healthcare data, since only the intended user can gain access.

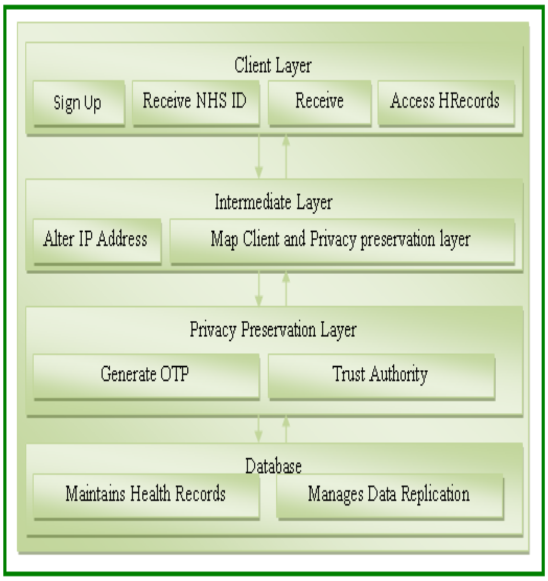

Fig 1: Overall System Architecture

Fig 1 depicts that the overall system has got three level of architecture. The client layer includes all the activities that are made by the client. The client or patient needs to sign up or enrol himself to the National Health System (NHIS). The NHIS is responsible for verifying the identity of the client, which can be achieved by adhaar card presently.

With the usage of Adhaar card, every single citizen of India can be distinguished as biometrics such as eyeball and fingerprints are taken into account.

After the verification of identity, NHS identifier will be issued to the client. The client can then use this NHIS_ID with the Health Service Provider (HSP).

Then after the patient is examined by the physician with the needed tests, the test results will get its room of storage in the local patient database.

Then the test results are transmitted to the NHIS cloud database. When the client needs to see through the data and when the client logs in with the NHIS_ID provided, another level of security is enforced.

A One Time Password is generated by the RSA security. For every minute a 6 or 8 digit random number is generated and is sent to the user's mail id. After providing the password, the user can gain access to the test reports. The intermediate layer modifies the IP address in order to reduce the degree of identity, in order to ensure privacy. However, the person can be identified. The intermediate layer maps the client with the privacy preservation layer.

The privacy preservation layer aims at providing OTP and the Trust Authority (TA) manages the security issues. TA has all the control over the system. TA has the role to provide privacy to the patient to certain degree and at the same time the person should be able to be identified.

The healthcare data are usually replicated in order to increase availability even when the natural disasters or system failures occur.

The replicas are needed to be managed very carefully, in the sense that if the parent record is modified, then all the corresponding replicas are needed to be modified. However, this is out of scope of this paper.

4. PROCESS FLOW

The overall process of this work is depicted in Fig 2.

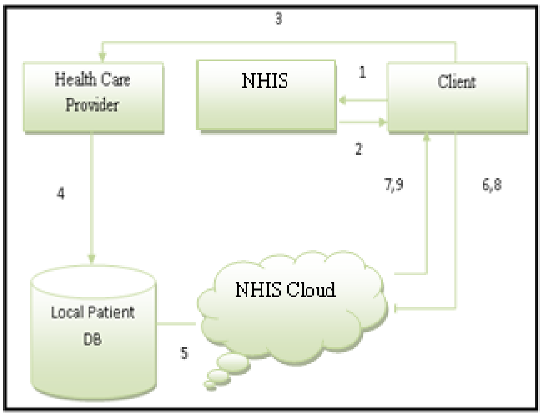

Fig 2: Process Flow of the System

Fig 2 depicts the process flow of the system. The numbers presented indicates the steps involved and are given below.

Step 1: A client enrols himself to the National Healthcare Info System (NHIS)

Step 2: The NHIS verifies the identity of the client with some standard proof and then an ID is allotted to the client.

Step 3: The client can now take the facility of hospitalization with the registered Health Care Provider.

Step 4: The client is examined with several necessary tests and the scanning or laboratorial results are stored in the local patient database.

Step 5: Now, the stored reports are submitted to the NHIS cloud database.

Step 6: The client requests access from the NHIS, in order to look into the test reports being submitted by the Health Care Provider.

Step 7: The NHIS sends a One Time Password (OTP), which can be of 6 or 8 digit random number to the client's email.

Step 8: Now the client is expected to provide the OTP in the corresponding place.

Step 9: After successful matching of OTPs the client is given access to the health records.

5. CONCLUSION

This work is developed with three layers. Privacy is provided in this work by providing OTP which is generated by the privacy preservation layer. The OTP is 6 or 8 digit randomly generated number by RSA. In future, this work may get enhanced in the aspects of providing effective mechanism for data updation.

6. REFERENCES

[1] Rolim CO, Koch FL, Westphall CB, Werner J, Fracalossi A, Salvador GS. A cloud computing solution for patient's data collection in health care institutions. In: Proceedings of the 2nd International Conference on eHealth, Telemedicine, and Social Medicine; February 10-16, 2010; New York, NY: IEEE. 2010. Feb 10

[2] Nkosi MT, Mekuria F. Cloud computing for enhanced mobile health applications. Proceedings of the 2010 IEEE 2nd International Conference on Cloud Computing Technology and Science (CloudCom); The 2nd IEEE International Conference on Cloud Computing Technology and Science; Nov 30- Dec 3, 2010; Indianapolis, USA. New York, NY: IEEE; 2010.

[3] Rao GSVRK. Sundararaman K, Parthasarathi J. Dhatri: a pervasive cloud initiative for primary healthcare services. Proceedings of the 2010 14th International Conference on Intelligence in Next Generation Networks (ICIN); The 14th IEEE International Conference on Intelligence in Next Generation Networks (ICIN); October 11-14, 2010; Berlin, Germany. New York, NY: IEEE; 2010.

Koufi V, Malamateniou F, Vassilacopoulos G. Ubiquitous access to cloud emergency medical services. Proceedings of the 2010 10th IEEE International Conference on Information Technology and Applications in Biomedicine (ITAB); The 10th IEEE International Conference on Information Technology and Applications in Biomedicine (ITAB); November 3-5, 2010; Corfu, Greece. New York, NY: IEEE; 2010.

[5] Wang X, Tan Y. Application of cloud computing in the health information system. Proceedings of the 2010 International Conference on Computer Application and System Modeling (ICCASM); International Conference on Computer Application and System Modeling; October 22-24, 2010; Taiyuan, China. New York, NY: IEEE; 2010.

[6] He C, Jin X, Zhao Z, Xiang T. A cloud computing solution for hospital information system. Proceedings of the 2010 IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS); IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS 2010); October 29-31, 2010; Xiamen, China. New York, NY: IEEE; 2010.

[7] Yang CT, Chen LT, Chou WL, Wang KC. Implementation of a medical image file accessing system on cloud computing. Proceedings of the 2010 IEEE 13th International Conference on Computational Science and Engineering (CSE); The 13th IEEE International Conference on Computational Science and Engineering; December 11-13, 2010; Hong Kong, China. New York, NY: IEEE; 2010.

[8] Guo L, Chen F, Chen L, Tang X. The building of cloud computing environment for e-health. Proceedings of the 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies (EDT); The IEEE International Conference on E-Health Networking; July 1-3, 2010; Lyon, France. New York, NY: IEEE; 2010.

[9] Zhang R, Liu L. Security models and requirements for healthcare application clouds. Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD); The 3rd IEEE International Conference on Cloud; July 5-10, 2010; Miami, FL, USA. New York, NY: IEEE; 2010.

[10] Kudtarkar P, Deluca TF, Fusaro VA, Tonellato PJ, Wall DP. Cost-effective cloud computing: a case study using the comparative genomics tool, roundup. Evol Bioinform Online. 2010;6:197–203. doi: 10.4137/EBO.S6259.

[11] Vaquero LM, Rodero-Merino L, Caceres J, Lindner M. A break in the clouds: towards a cloud definition. ACM SIGCOMM Comput Commun Rev. 2008 Jan;39(1):50–55. doi: 10.1145/1496091.1496100.

[12] Sittig DF, Singh H. Eight rights of safe electronic health record use. JAMA. 2009 Sep 9;302(10):1111–3. doi: 10.1001/jama.2009.1311.302/10/1111

[13] Zhang R, Liu L. Security models and requirements for healthcare application clouds. Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD); The 3rd IEEE International Conference on Cloud; July 5-10, 2010; Miami, FL, USA. New York, NY: IEEE; 2010.

[14] Microscoft Corp. 2010. Nov, [2011-09-07]. webcite Privacy in the Cloud: A Microsoft Perspective http://www.microsoft.com/privacy/cloudcomputing.aspx.

[15] Wang J, Zhao Y et al. (2009). Providing Privacy Preserving 1. in cloud computing, International Conference on Test and Measurement, vol 2, 213–216.