VOL. 10, NO. 10, JUNE 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

A NOVEL METHOD OF SECURITY AND PRIVACY FOR PERSONAL MEDICAL RECORD AND DICOM IMAGES IN CLOUD COMPUTING

C. Gunamalai[1] and S. Sivasubramanian[2]
[1]Bharath University, Chennai, India
[2]Dhanalakshmi College of Engineering, Chennai, India
E-Mail: malainathan@yahoo.com

ABSTRACT

Cloud computing is a emerging technology that allows us access the shared resources which was stored in the cloud data center. Several healthcare centers store the patient's Personal Medical Record and DICOM (Digital Imaging and Communications in Medicine) images in the cloud data center. Using cloud data center healthcare center would benefit of low cost, availability and disaster recoverability. The main idea of this paper is the various healthcare centers from different places can easily access and use the patient's information for their treatment. Healthcare center and registered in the outsourcing organization in the cloud. This outsource organization provide access right to registered health care centers through Two Way Authentication. First step is a conformist one where the user enters his user id and password, if it matches with the stored database of the cloud then they proceed of authentication, the second step is the database triggers an application which generates a dynamic password. This pass word is sent to the user on his personal mobile as a message or an e-mail. The second security method is Column Based Encryption (CBE). Using CBE, access policies are expressed based on the attributes of handlers or data, which enables a health center to selectively share their Personal Medical Records and DICOM image among a set of users by encrypting the file under a set of attributes or columns.

Keywords: DICOM, CBE, two way authentication, PMR, AA, PBU, PEU.

1. INTRODUCTION

Cloud computing is an emerging technology that allows us access the shared resources from anywhere and anytime by using internet. Several healthcare providers and insurance companies registered with outsourcing organization and store the patient's medical data in the form of Personal Health Record and DICOM images. DICOM stands for Digital Imaging and Communication in Medicine. The DICOM standard was created by the National Electrical Manufacturers Association (NEMA), and it also addresses distribution and viewing of medical images. The DICOM file consists of a header, followed by pixel data. The header comprises of the patient name and other patient details, the pixel data consist of MRI, X-Ray, and CT scan images mostly used in Radiology examination which can be read by a DICOM reader. It is an essential way for storing patient's medical records electronically.

Patient has various healthcare center including physicians, specialists, therapists, and other medical practitioners. Therefore, a healthcare provider may request a patient's records from other healthcare center through outsourcing organization; this common place could facilitate and enhance this sharing of data among different healthcare center more efficiently.

Due to the vast amount of medical image and data that needs to efficiently stored, retrieved in the cloud and the increased security coercion that explicitly have to be addressed. Embedding patient information into a DICOM header through data hiding could improve the level of security. Such security provides integrity of DICOM images and corresponding documentations.

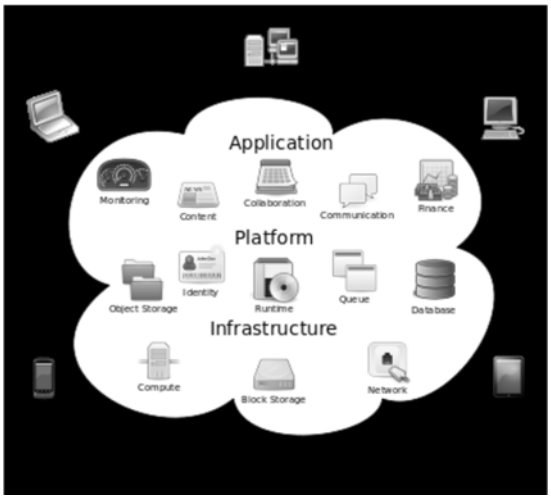

Figure-1. Cloud architecture.

The scheme undetectably embeds in medical images patient's information like name and unique identification number. Anytime and anywhere access to medical images and instant retrieval of DICOM images and data of any ethics with a cloud-based image storage and management service using standard DICOM protocol. Security service is an essential pillar of DICOM Standard and cloud computing system management. Security is including confidentiality, the reliability of stored information and consistency, essential to cloud-based medical imaging solution. It allows access, sharing,

exchange and viewing of DICOM images from virtually anywhere. The cloud computing promises lower cost, high scalability, availability and disaster recoverability which can be a natural solution some of the difficulties we met for long term medical image archive [7].

No need of any other devices DICOM data feeds [8]. This paper discussed how to achieve security for DICOM images and records in the Cloud. We proposed the two methods to provide the security for the DICOM images and PHR first is Two Way Authentication (TWA) and Column Based Encryption (CBE).

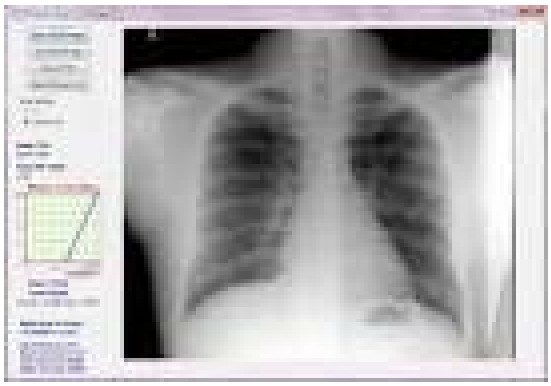

Figure-2. DICOM images.

2. FUNCTIONS AND IMPLEMENTS

As mention above, we provide two functions: Two Way Authentication (TWA) and Column Based Encryption (CBE).

A. Two way authentication

In the conventional authentication process there might be illegal use of data if the password is disclosed to a unfamiliar person. Authentication is a technique of identifying the user who poses the right to access, alter and update data stored on cloud. In general the authentication process is done using a unique login id and a password. If the id and password match with the database of the previously saved then the user is authentic and he can access it according to the privileges set for them. To overcome this we introduce an idea of Two Way Authentication where the process takes place in two steps. The first step is the healthcare center enters their user id and password which was allotted from outsourcing organization, if they match with the database of the cloud data center then they proceeds to second step of authentication. The first step is describing bellow.

Welcome To Cloud

Username:

Password:

Sign in

In the second step the database triggers an application which generates a dynamic key. The generated key is sent to the particular healthcare center on their personal mobile as a text message or an e-mail which they was chose. Now the user needs to enter that dynamically generated key within a preset time period after which the key expires. If the healthcare center enters the key correctly and matches with the key sent to them then the process of authentication is completed.

Welcome To Cloud

Cloud Token:

Sign in

a) Issues with two way authentication

Though Two Way Authentication gives us advanced security in identifying a healthcare center, the main difficulty would be the time that it takes to create a dynamic key and again compare it with its stored database. It is a tiresome process and needs extra application software to maintain it. In addition every time it follows the same process for each and every user and for each and every login [7]. The initial process of authentication is as shown in Figure. After entering username and password they are comparing with the database in the stored database in the cloud. If they are authentic then a dynamic key is generate individually with an expiry session connected with it. They are communicating to the user through a text message sent to his mobile or an e-mail. The user then enters them and if they again match with the sent key and they gets access to the database stored in the cloud.

B. Column based encryption

In this paper, we try to study the secure sharing of Personal Medical Records and DICOM images stored on cloud servers, and focus on complicated and challenging key organization issues. In order to protect the Personal Medical Records (PMR) and DICOM image stored on a cloud server, we implement Column Based Encryption (CBE) as the main encryption method. Using CBE, access policies are converse based on the attributes of Healthcare Center or data, which enables a Healthcare Center to selectively share their PMR and DICOM image among a set of Healthcare center by encrypting the PMR and DICOM image under a set of attributes, without the need to know a whole list of Healthcare center. Earlier to storing the records in cloud server, they are encrypted using any encryption algorithm which ensures the

patient's full control over their PMR and their DICOM images. Healthcare center only decide which authenticated users can access which set of files. Personal Medical Record is an internet based request that permits people to access and organize their lifelong PMR information and make if suitable parts of its accessible to those who require.

a) PMR and DICOM image owner and Database authority

PMR owner and database authority is the registered healthcare center in the cloud data center through outsourcing organization. The main goal of our structure is to give secure Healthcare center-centric PMR right to use and successful key administration at the same time. The main idea is to split the system into various security domains namely, Public Users (PBU) and Personal Users (PEU)) according to the different users' data access requirements. The Public Users consist of users who make right to use based on their roles, such as doctors, physicians, specialists, therapists, insurance companies, researchers.

A PBU can be mapped to a self-governing sector in the society, such as the registered Healthcare Center, Government and Insurance sector. For every PEU, its users are personally associated with a data owner that is Healthcare Center. Other healthcare Center makes accesses to PMR and images based on access rights assigned by the particular Healthcare center or data owner. Each data owner (e.g., Healthcare center) is a trusted authority of their own PEU, who uses a CBE system to control the secret keys and access rights of users in their PEU. The owner grants access rights on a patient basis, if the patient is admitted other healthcare center, the data owner gives the access right to the particular healthcare center to continue their treatment.

b) Cloud server

We consider the server to be public cloud server, i.e., honest but inquisitive. That means the server will try to get as much secret information in the stored PMR files and DICOM images as possible, but they will really follow the procedure in common. Some hackers will also try to access the files their rights. For example, a pharmacy may want to obtain the prescriptions of patients for and boosting its market and profits. The other possibility is the insurance sector agent may try to access. In addition, we assume each Healthcare Center in our system is save their PMR and images with a public/private key pair and entity validation can be done by usual challenge-response protocols.

c) Column based access

We decided to use the granule of table columns and store Medical data which is sensible with different keys that depend on the job. Access Control List (ACL) rules to apply to the different Healthcare center and their staff. In this ACL include such as system administrators, doctors, therapist and other Healthcare center. Hence, it is necessary to table columns each professional needs access to, key to-role relation is N-to-M because different roles may access the same column, and the key management maintains those links together with encryption keys.

In the following we report an example to understand the Column based access. We assume that cloud database has only four columns in the table called Table-1. As in Figure-4, the Table-1 has 4 columns: Column1, Column2, Column3, and Column 4. The data in Column1 is decrypted with the encryption key Key1, and data in Column2, Column3 and Column4 with Key2, Key3 and Key4, respectively. User1 is part of in the Doctor or health care staff, while User2 is in the Accounting Manager, User3 is the Medical Insurance Staff, and User4 is registered other Healthcare center. According to their roles, our system grants User1, User2, User3 and User4 different keys.

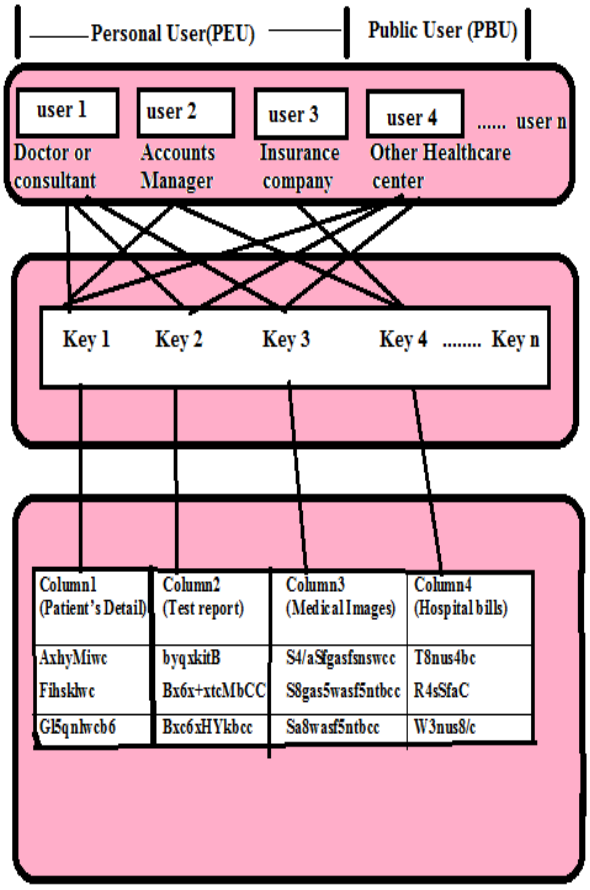

Figure-3. Users access multiple column.

User 1 can decrypt Column 1, Column 2, and Column3 that contain patient's details, medical record or test report and DICOM images, User2 can decrypt Column1 and Column4 that contain Patients detail and healthcare center bill, User 3 can decrypt medical record or test report and DICOM images contains to know the

patient's medical history it will be diagnose and treat the patient. The medical bills to quantify the medical expenditure the patient has to pay. User 4 can decrypt data in Column 1, Column 2, Column 3 that c patient's details.

3. CONCLUSIONS

In this paper, we have proposed a novel frame of secure distribution of PMR and DICOM images in cloud data center. We assure the security and privacy including confidentiality for the PMR and DICOM image in the cloud database by trusted outsourcing organization. We achieve this security reliability by TWA and CBE procedure. Healthcare center shall have complete control of their own privacy through encrypting their PMR and images files to allow granule access. This paper introduce the unique confront brought by multiple PMR owners and users, in that we significantly reduce the complication of key administration while enhance the privacy assurance compared with previous works. So that the healthcare center can allow access not only by their own staff, but also various users from public domains with different professional roles like government staff and other healthcare center staff.

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, -Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings, Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (Secure Comm '10), pp. 89-106, September 2010.

[2] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, -Securing the E-Health Cloud, Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, -Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing, Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

[4] The Health Insurance Portability and Accountability Act, 2012.

[5] Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them, ‖ http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6] A. Bischoff-Grethe, B. Fischl, I.B. Ozyurt, S. Morris, G. G. Brown, C. Fennema-Notestine, C. P. Clark, M. W. Bondi, T. L. Jernigan, *et al*, "A technique for the de identification of structural brain MR images"

[7] Oleg S. P ianykh, "Digital Imaging and Communications in Medicine (DlCOM), A Practical Introduction and Survival Guide ", book published by Springer-Verlag Berlin Heidelberg, pp. 247-261, 2008and 2012.

[8] National Electrical Manufacturers AS9) ciation, "DlCOM Part 8: Network Communication Support for Message Exchange", PS 3. 8-2011, pp-10-25.