International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-6)

Research Article | June 2014

Security issues of Patient Health Records in E-Hospital Management in Cloud

Jitendra Madarkar
SCSE VIT University
India

Anuradha D
SCSE VIT University
India

Sachendra Waghmare
SCSE VIT University
India

Abstract-

Cloud computing is generally a distributed computing over a network. Cloud computing is one of the growing computing technologies in distributed paradigm. Even though technology is growing rapidly but any unauthorized user can exploit the vulnerability of cloud computing system. Different types of approaches are in progress to protect the privacy of this system. In this paper we used efficient encryption algorithm to secure E-Hospital management in cloud and provide segmentation to keep confidential medical image in cloud. For reducing image size we used Hadoop and MapReduce.

Keywords: PHR- Patient Health Record, cloud service provider, Wireless sensor network, ABE- Attribute –Base Encryption. Trusted Privacy Domain (TPD).

I. Introduction

Cloud computing is the next development of distributed computing image which provide**s** resource (sever, application, storage, services) to cloud consumer. It is consolidation of conventional technologies and network technologies such as parallel computing, grid computing, distributed computing, network storage technology, load balancing and virtualization. The general idea of cloud computing is to enhance the performance of the cloud in order to reduce load on consumer side. The main key characteristics of Cloud computing is shown in the following [13]: Cost Effective, on-demand self service, Ubiquitous network access, Rapid Elasticity, High reliability, Versatility.

In cloud computing performance, availability and security are main research topics. Among them cloud computing security is one of the important research topic. [11] Cloud computing deploy resources and monitors the usage of resources all at times. Cloud computing collects the information, resources and also provides services to millions of users simultaneously. In this paper we did survey on security of E-Hospital management**.**

A now day's E-hospital record becomes most important in many countries. There are much standardization putting effort on data exchange and interoperability. E-hospital record provides various applications regarding medical research, accounting, billing and trading intellectual property. E-Health Record decrease human workload, hospital cost and improves personal health management. Due to 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. There are several legal penalties for violating privacy laws. If E-health data is leaked outside the cloud accidentally the IT provider would have to face legal penalties.

II. Related work

E-hospital Cloud security challenges:

Cloud service provider provided service to multiple E-Hospital record providers. E-hospital record provider utilized records from virtualized pool that provided by cloud service provider. Usually cloud is associated with number service provider and number of service consumer due of there may be high security concern. A healthcare provider can use private cloud in its premises to monitor proper security policies and access control E-management and control for identity. However in case of public cloud, it is very important to provide cloud services which support security mechanism to secure the transfer of E-hospital data to and from client and cloud service provider. In multi-tenant cloud where data stored along with other E-hospital healthcare providers so there is need of security to keep data secure. We have to make sure that the service provider itself can't use or access the E-hospital record. To avoid the leakage of the data there is need for efficient security mechanism for the E-Hospital cloud [3]. There are several ways to apply strong security measure, but they enforce high computation and communication cost forcing them in cloud. In addition, another issue is Cloud service may not be get fully reflected about organization security requirements and policy.

Now days in hospital Patients monitoring done by using sensor network it help to gather health record. This approach provides security for confidentiality, data integrity and fine access control. In order to realize the above objectives,

author [16] describes an architecture shown in figure. 1. In this architecture author takes two types of users, patients and healthcare professionals. Considering the following factors: 1. Wireless sensor network contains the health information from patients monitoring 2.authentic healthcare professionals only can access store data.3. HA (health Authority) imposes and specifies the security policies of health care institution our architecture offers virtually infinite storage capacity and high scalability. To achieve fine-grained access control, attribute based encryption (ABE) is used to encrypt data before storing them. The cipher text (encrypted data) can be decrypted by any user if his secret key satisfies the access policy. To tackle the first challenge of ABE integration, both symmetric cryptography and ABE are used. Mostly, each file is encrypted with a randomly generated symmetric key (RSK) and RSK is again encrypted with ABE. Both the encrypted file and the encrypted RSK are sent to the cloud for storage to allow fine grained access.

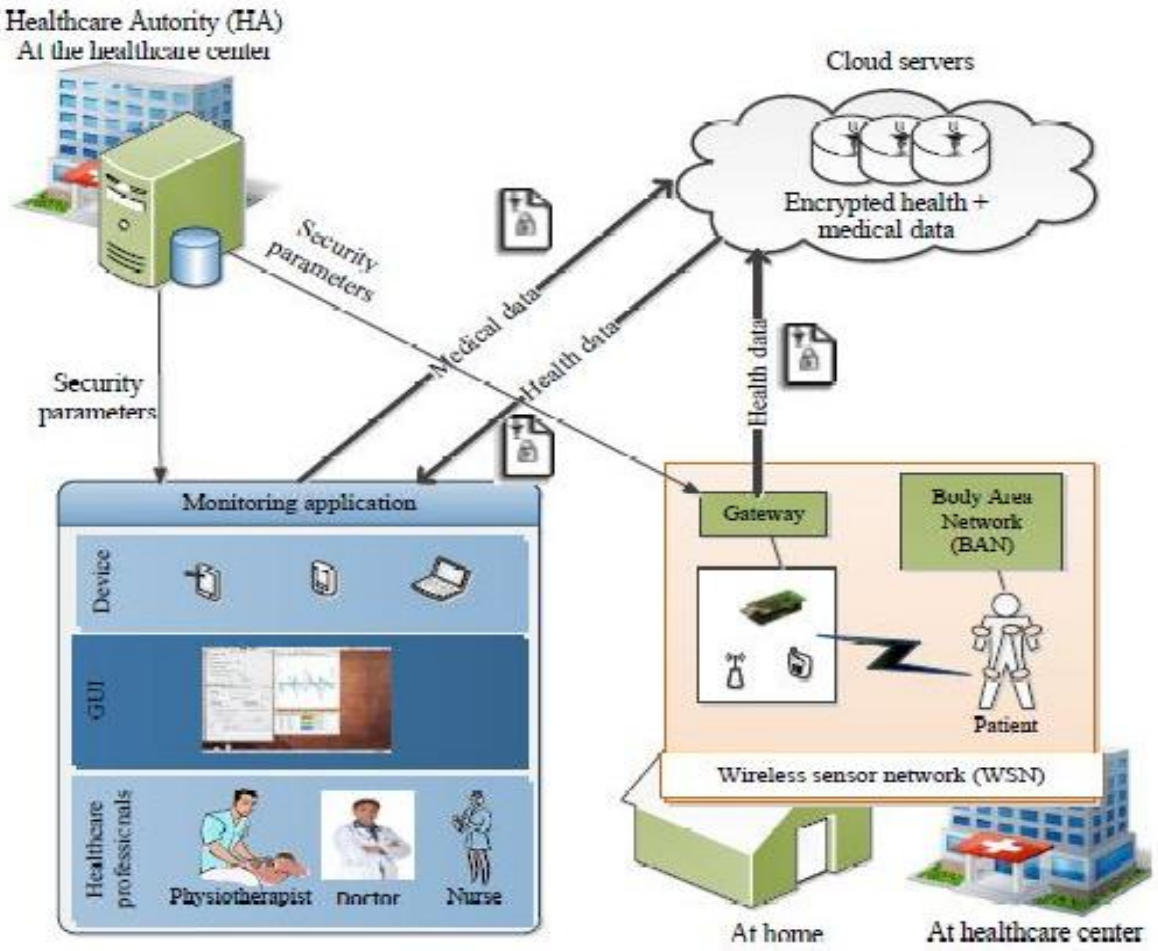

Fig1.Cloud based Architecture [16]

In this architecture, each patient has a personal WSN composed of a set of lightweight/small sensor nodes and a gateway. A WSN enables continuous health monitoring of the patient at the hospital and at home. Sensor nodes are used to collect different health data such as heart beats, motion and physiological signals. Each sensor node sends the collected information via wireless communication channel to the gateway. The gateway compiles the different health data into a file and then encrypts it using the RSK. Thereafter, it sends the final encrypted file using the access structure obtained from the HA to the cloud.

In the given architecture [16] of cloud server, PHR user, PHR owner and third party Auditor are the main entities. In cloud where owner can stored the data of PHR and owner can share his data with his friends, Doctor and family member. PHR owner has right to do something on a data. PHR user is associate person and user has rights consorting to their position with PHR owner. Cloud server is storage where owner can store sensitive clinical data. [16] Third party auditor provides security to access cloud storage on the behalf of PHR owner upon request. There is no conspirator between TPA and with either owner or cloud servers during the auditing process because TPA is reliable and independent. Without any additional online burden of data owners and without local copy of data TPA can be efficiently audit the cloud storage. Auditing protocol avoid the leakage of an owners outsourced PHR toward TPA. Outsider attackers have capability to attack on cloud storage services and latter on it can delete owner's data while remaining undetected.

Encryption algorithm:

1. Function or key generation -generate two keys i.e. private key and public 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 ciphertext C of f (p).

Decrypt (private P) = f (p)

f can be any arbitrary function then scheme becomes Homomorphic and Eval of ciphertext is compact. Complexity function f is independent on size. The Eval algorithm evaluates its own decryption algorithm. Utilizing Homomorphic Authenticators reduce arbitrarily communication overhead for public audit ability without introducing any online burden on the data owner, due to of author resort Homomorphic authenticator technique.

One approach is to allow PHR owner patient to access PHR data from cloud by selective sharing to avoid risk of confidential exposure [20]. Rather 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 Patient wants to reject access of other users, patient can. This model helps to create patient-centric PHR system 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 "break-glass access to PHR." However some communication overhead during key distribution and health record management or user management, 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]. This can be achieving through utilizing combined advanced cryptographic technique: lazy re-encryption, proxy re-Encryption (PRE) and Key-Policy Attribute-based Encryption (KP-ABE). Each record signifies a set of defined attributes and each user is assigned an accessed structure. For this attribute-based access control, KP-ABE is used to guide encryption keys of recorded data. Data owner controls computation operations with confidentiality to cloud owner by combining PRE &KP-ABE. As a result cloud owner can't decipher any "plaintext medical data." By this methodology, scalability is also achieved using a lazy re-encryption technique to allow cloud owners to combine the computation tasks of multiple system operations. This causes the computation complexity to be either "proportional to the number of system attributes", or "linear to the size of the user access tree".

Trusted privacy domain (TVD) for the patient's health record

In [21] provide technical solution about security issue of external storage and end user platform. User uses their platform for accessing not only health record but also other application. Therefore due to lack of security with in platform or operating system, end user platform become very defend less to malware attacks which can obtain the users secret data and password. This is in addition to the issue of transferring medical data to mobile storage units which take them away from any security control in the Cloud. In this [8] paper author approach proposes constructing trusted privacy domain (TVD) for the patient's health record. End user System capable to divide the execution environment for application into different domain and it isolate from each other. Health record is kept in TVD that is accessed only by authorized users. Security architecture and TVD infrastructure helps to prevent data leakage. The system automatically encrypts data stored in external storage with privately accessible keys when health record stored on external storage. A security gateway to control the data export under a data protection protocol when exporting data to external system that are not connected to the TVD.

TVD infrastructure is mostly known for automatic management which verifies integrity of client platforms, when they try to join a TVD and then distributes keys and a policy in which TVD establishment; key management and policy enforcement which is securely handled by kernel are transparent to users. Connection between different platforms is secured through an IPSec-secured virtual private network. The approach imply on the end user platform that it contain a security hardware module such as the trusted platform Module (TPM). This all cases used in devices that used by patients. This approach increases concern about the scalability and complexity due to enforced on the client platform of the E-hospital providers and privacy domain is established in the cloud.

Many methods have been proposed for E-hospital record security but till now there is no such method for image encryption. Conventional encryption algorithm such as RSA, AES and DES are not used that much for image encryption because they required high computational power. Size of image is directly proportional to the computing resource. In addition when using one of the above algorithm on text then the original text size should be equal to the decrypted text size where as in case of image little distortion or loss acceptable. For image decrypted and encrypted impose large burden on cloud resource. If we do CT scan or image captures by camera the size of image is so large due that it require so much space in cloud to avoid this we approach [5] image conversion model.

III. Proposed idea

In this paper we apply efficient lightweight encryption algorithm. The main goal is to provide encrypted E-hospital record in cloud. It took some time to encrypt or decrypt the data so that only sensitive E-hospital records are needed to be encrypted. The TSFS algorithm used for numeric and characters but in E-hospital record we also need to store image in cloud and it should be encrypted form. For that we are going to apply TSFS algorithm, segmentation for image and image reduction using Hadoop and MapReduce.

TSFS algorithm provides four type of transformation: 1.transposition, 2.substitution, 3.Folding and 4.Shifting. Transposition and substitution are most important kernel technique to construct symmetric encryption algorithms. Each has two factors of security and cryptology, confusion and diffusion. In this algorithm substitution and transposition cipher techniques use mostly. The given above four techniques of transformation use for decryption and encryption. In this algorithm encryption is referred as inverse of decryption. This algorithm is said to be a non Feistel cipher means each transformation must be invertible. The inverse cipher and cipher operation must be canceling to each other. The key keys should be in reverse order.

1. Transposition
   Transposition changes the location of the content or symbol. A symbol of the 2^{nd} position may be shifted to the 10^{th} position.
2. Substitution
   Substitution cipher is used to change the symbol with another. We replace symbol 0 with symbol 9. The substitution cipher is classified into two type a. Polyalphabetic cipher b. Monoalphabetic cipher. Monoalphabetic substitution follows one-to-one relation between symbol in plaintext and symbol in ciphertext. And Polyalphabetic substitution follows one-to-many relationship between symbols in plaintext and symbol in ciphertext. Here we are using modified affine cipher for encryption. Affine cipher is combination of multiplicative cipher and additive cipher. For this we used two keys one for multiplicative cipher and another for additive Cipher.
   Encryption process is done by
   Ciphertext (C) = (P * k1+ k2) mod M
   Decryption process is done by
   $$\text{Plaintext (P)} = ((C - k2) * k1^{-1}) \bmod M$$
   If the key k1 and M are co prime then only multiplicative inverse of k1 exists. Key domain for any multiplicative cipher must be in the range from 0 to 26
3. Folding
   The folding techniques take an input as result of substitution. It one of the transposition ciphers, just like the paper fold, the matrix is folded vertically, horizontally and diagonally. The folding technique mixes the data from one position to another position.
4. Shifting
   Shifting cipher provides a simple way to encrypt and decrypt numbers by using 16- array element of numeric digits. Each element contains numeric characters from 0 to 25. Each digit must appear in any order but only once in each element of the array. The input for encryption of this cipher is the result of the folding cipher which replaces each digit of the number by its position within its array element. For decryption the position is given as an input, based on which data is taken and that data is plaintext of the given cipher text.

We can keep confidential medical image on entrusted cloud by using segmentation [2]. It shuffles the pixel of medical image by using Arnold Cat Map (ACMap) [19]. Then resulting image splitting into several small pieces with different title and stored in cloud. The splitting image metamorphoses into a jigsaw puzzle because the title of splitting image unknown to cloud service provider holding the different titles. It is difficult for unauthorized user to reconstruct full image because of pixel shuffling.

Reducing the size of medical image with help of Hadoop and MapReduce

Pass platform consist of social common algorithms library (social media data analysis platform), cloud Infra Management platform, data processing and cloud distributed. Firstly, social common algorithms library are analyze relationship between users, usage pattern and health record on demand, and it provide the function of Transcoding , Transmoding, decoding and encoding as the form libraries. Transmoding means converting one image file into file in terms of file size. Transcoding helps to converting one image file into files suitable for numerous digital devices in terms of file form. Secondly this approach able to store E-health record by applying Hadoop Distributed files System (HDFS), Google MapReduce and Hadoop Database System (Hbase) on cloud. Lastly cloud Infra Management platform contain the concept of cloud infra Management, green IDC and cloud QoS [4]. Hadoop helps to conduct Transcoding and Transmoding processes are as fallows. First of all health care provider created image is automatically distributed and stored in each node running on HDFS. Later MapReduce convert stored medical image datasets on HDFS by performing batch processing. Lastly each node executed simultaneously on image database.

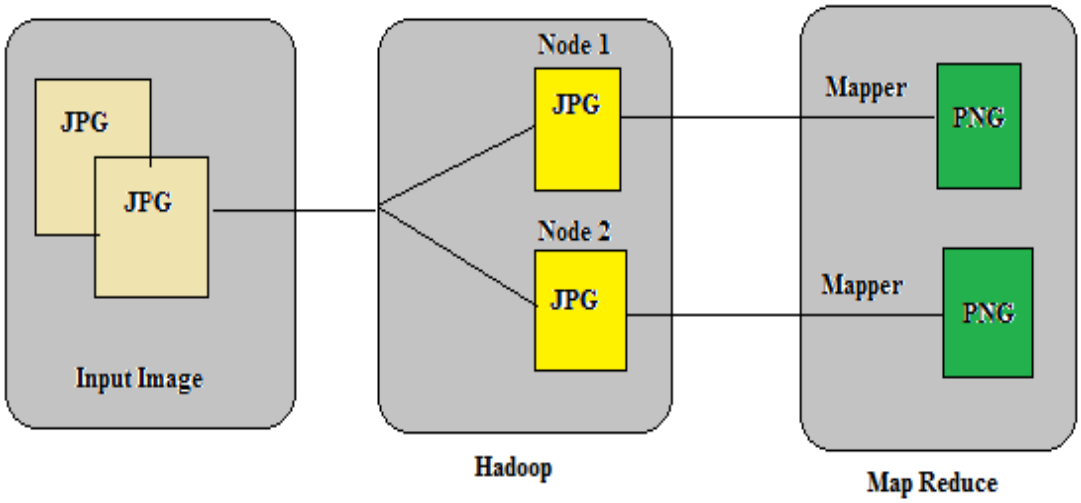

Fig 2 . Image conversion module

Prototype:

The above figure 2 shows image conversion module. The above converter helps to convert uploaded medical images by health care provider into proper file format and size suitable for E-hospital users devices in real time using elastic computing resource, MapReduce programming and HDFS. Up loader have different option such as resolution size and scale so user can select these option during image conversion module.

IV. Conclusion

In this paper we discuss about security of E-hospital management in cloud computing and image conversion model. Now days healthcare is important topic in cloud computing but it is very defend less toward security. Here we propose TSFS algorithm which very lightweight efficient encryption algorithm. It helps to maintain confidentiality of healthcare data. Medical image is very large in size so it required so much space in cloud. To avoid this we use image conversion model to reduce the size of image by using Hadoop and MapReduce.

References

[1] Eman AbuKhousa, Nader Mohamed and Jameela Al-Jaroodi," e-Health Cloud: Opportunities and Challenges", *Future Internet* 2012, *4*, 621-645;

[2] Arash Nourian, Muthucumaru Maheswaran," Using segmentation for confidentiality aware image storage and retrieval on clouds", Globecom 2012 - Communication and Information System Security Symposium.

[3] D.Manivannan1, R.Sujarani2,"Light Weight and Secure Database Encryption Using TSFS Algorithm",

[4] Jung ho Eom and Min woo Park" Design of Internal Traffic Checkpoint of Security Checkpoint Model in the Cloud Computing", International Journal of Security and Its Applications Vol. 7, No. 1, January, 2013.

[5] Palivela Hemant, Nitin.P.Chawande, Avinash Sonule, Hemant Wani," DEVELOPMENT OF SERVERS IN CLOUD COMPUTING TO SOLVE ISSUES RELATED TO SECURITY AND BACKUP", 978-1-61284-204-2/11/$26.00 ©2011 IEEE.

[6] Akhil Behl," Emerging Security Challenges in Cloud Computing", 978-1-4673-0126-8/11c 2011 IEEE.

[7] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou" Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011.

[8] *Kevin Hamlen, Murat Kantarcioglu, Latifur Khan,"* Security Issues for Cloud Computing*",* International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010.

[9] Priyank Rajvanshi, Varun Singh Nagar, Priyanka Chawla, "Data Protection in Cloud Computing", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-3, August 2013

[10] Uma Somani, Kanika Lakhani, Manish Mundra," Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[11] Zhang Xin, Lai Song-qing, Lai Nai-wen," Research on Cloud Computing Data Security Model Based on Multi-dimension" 978-1-4673-2108-2112©2012 IEEE.

[12] Miika Komu, Mohit Sethi, Ramasivakarthik Mallavarapu, Heikki Oirola and Rasib Khan," Secure Networking for Virtual Machines in the Cloud", 978-0-7695-4844-9/12 © 2012 IEEE.

[13] Ziyuan Wang," Security and privacy issues within the Cloud Computing", 2011 International Conference on Computational and Information Sciences.
[14] Pengfei You, Yuxing Peng, Weidong Liu, Shoufu Xue," Security Issues and Solutions in Cloud Computing", 2012 32nd International Conference on Distributed Computing Systems Workshops.
[15] Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah and Yacine Challal,"Secure and Scalable Cloud-based Architecture for e-Health Wireless sensor networks",
[16] 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).
[17] Dr. W. Liu, Dr. E.K. Park." e-Healthcare Cloud Computing Application Solutions: Cloud-enabling Characteristices, Challenges and Adaptations", 2013 International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium.
[18] Cong Wang, Qian Wang, and Kui Ren," Ensuring Data Storage Security in Cloud Computing", 2009 IEEE;
[19] V. I. Arnold, Mathematical methods of classical mechanics, 1978.
[20] 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.

