International Journal of Multidisciplinary Research and Development

International Journal of Multidisciplinary Research and Development

Volume :2, Issue :4, 416-420
April 2015
www.allsubjectjournal.com
e-ISSN: 2349-4182
p-ISSN: 2349-5979
Impact Factor: 3.762

Ghodake Shubhangi
Computer Engineering,
S.K.N.C.O.E.PUNE,
Maharastra, India

Joshi Priyanka
Computer Engineering,
S.K.N.C.O.E.PUNE,
Maharastra, India

Khobragade Pranjali
Computer Engineering,
S.K.N.C.O.E.PUNE,
Maharastra, India

Chandak Manjiri
Computer Engineering,
S.K.N.C.O.E.PUNE,
Maharastra, India

Correspondence:
Ghodake Shubhangi
Computer Engineering,
S.K.N.C.O.E.PUNE,
Maharastra, India

Scalable and secure sharing of data in cloud computing using attribute based encryption

Ghodake Shubhangi, Joshi Priyanka, Khobragade Pranjali, Chandak Manjiri

Abstract
Each and every hospital provides personal health record to their patients. These records are provided to patient and only patient should have full access to it. It should decision of patient to whom he want to show his PHR and to whom not. A PHR service allow patient to create, manage and control his personal health data. As these records normally prepared and shared by third party services so there is so much chance of privacy and security risk. Also If any patient want to share his PHR only to his doctor from specific hospital, he can't share it privately only to him. Develop system for Scalable and secure sharing of data in cloud computing using Attribute Based Encryption which will store PHR data of patients with functionality of accessing and generating report in secure and authenticated way. Patient can have only and full control over his Personal Health Record. Patient or any User can decide with whom he wants to share his personal health record. Authorized person can check PHR details via HSN (Health Social Network) which will be our user interface for public and general access. Every data should be encrypted before reaching any third party like cloud services. Before handing reports to particular person or organization PHR will be encrypted with Attribution based Encryption (ABE) technique. We will use cloud service which will add additional features like security and scalability and efficiently.

Keywords: Personal Health Record, Health Social Network, Data Encryption Standard, Attribute Based Encryption

1. Introduction
Health is full of uncertainty. Patients are frequently in the dark about their condition, about their options, about what will happen to them. And even for the well informed, there is full of complexity and difficulty. Many patients and families report the frustrations of being passed from pillar to post, of being made to tell their story over and over again, of hospitals losing their notes. And also here is no privacy and Security on health records. Anyone can Access easily no such particular kind of security is there. Technology is now at a point where it can help us overcome these problems. People can go Online and request for their own records for viewing and accessing with security[1],[2].

In previous systems no such records in patients hand for accessing but now new emerging system is PHRs means Personal Health Record with Attribute-Based Encryption. Technology is now at a point where it can help us overcome these problems. People can go Online and request for their own records for viewing n accessing with security. In previous systems no such records in patients hand for accessing but now new emerging system is PHRs means Personal Health Record with Attribute-Based- Encryption. The lot of technology we can integrate in Cloud Computing. In cloud security is one of the problems. Cloud data should be secure for that we provide security. Medical Records are sensitive information. In cloud handling this medical records are very difficult. In cloud computing there is some security problem. So overcome the security threat while maintaining the medical records we need to improve the security level of the PHR system in cloud computing.

A Survey on Improving the Security of Public Health Record System in Cloud Computing**.** Attribute-Based-Encryption is technique for Encryption records with using attributes and keys. In internet data is store which should be in encrypted form because data is sensitive anyone can hack this data. There is some drawback of encrypting data i.e. we gave the private key to third party. We develop new Microsystems for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). In our

cryptologist, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.

2] Leterature Survey

The past and current information about health is collect, store and track, for this purpose we used toll called as PHR. By using this we can save our time and money as well as repetition of medical test should be avoided. A PHR is health record where all data about health is manipulated by patient itself. PHR is totally opposite to the current used electronic medical record. The electronic medical record is operated by different hospital and institution. The main purpose of PHR is to give the complete, good and correct summary of each patient's medical history and all this data is access via internet. PHR report mainly consists of lab result data from wireless result of patient data and patient data is collected from different hospital's computer[9].

A personal Health Record, or PHR, is a health record where health data and information related to the care of a patient is maintained by the patient. This stands in contrast to the more widely used electronic medical record, which is operated by institutions, such as hospitals and contains data entered by clinicians or billing data to support insurance claims[4].

The intention of a PHR is to provide a complete and accurate summary of an individual's medical history which is accessible Online. The health data on a PHR might include patient-reported outcome data, lab results, and data from devices such as wireless electronic weighing scales or collected passively from other devices like Hospital's computers. To realize the potential of PHRs and PHR systems to improve health and healthcare, significant steps are needed in the areas of privacy, security. Security is a critical component of a PHR system especially if it is accessible via the Internet. so according to survey of previous systems n health records can conclude that new systems are very well efficient and easy to accessible for patients use. In cloud computing we can combine the lot of technology. The main problem in cloud is security, for that purpose security is required when data is present in cloud. Handling the medical records in cloud is a very complex one[10].

There is the security threat in cloud computing. So overcome the security threat while maintaining the medical records we need to improve the security level of the PHR system in cloud computing. A Survey on Improving the Security of Public Health Record System in Cloud Computing[7].

3] Phr Solution Types

A] Paper-based PHRs

Personal health information is recorded and stored in paper format. Paper-based PHR consist of Printed laboratory re-ports, Hospital notes, and health data of each individual patient. Cost required is less, access without use of computer. The paper-based PHR is developed in 1980 and used for pregnancy record. It is difficult to update, share with other. Paper-based PHRs are concern to physical loss [8].

B] Electronic device-based PHRs

Personal health information is recorded and saved in personal computer-based software that may have the capability to encrypt, and import data from other authority such as a hospital. PHR software can provide more sophisticated features such as data encryption, data importation, and data sharing with health care providers. Device such as a CD-ROM, DVD, smart card, or USB flash drive used for copying health record[8].

C] Web-based PHR solutions

Web-based PHR solutions are similar electronic device PHR solutions. The advantage of web-based solutions is that it can be easily combine with other services. For e.g. Medical data imported from other sources. Patients allow for data sharing with external authority [8].

4] Present System

In previous systems PHR is available publically. That means anyone can access data without taking any type of permission from patient. Patients don't have any type of control over his records. Technique used now is not reliable and secure because reporting is done by third party companies. In this system PHRs are stored publically no security is there so there are number of resources that can access patients record easily because no privacy and security is there[6].

Resources are from which patient's information can get easily like hospitals, school nurse, specialist doctor, payer data center, primary doctor, lab, pharmacy, LIC policies etc. so these are the resources from which patients data can be misplaced.

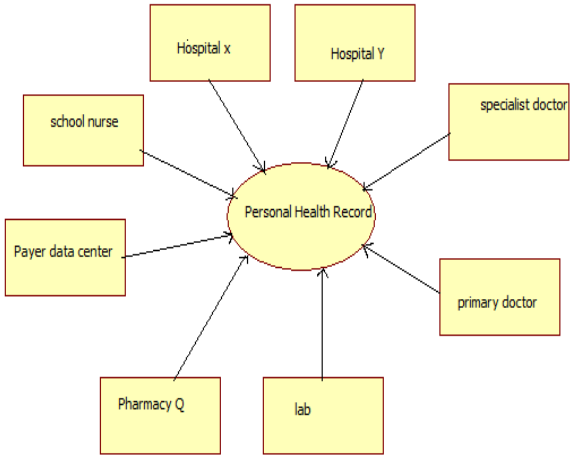

Fig 1: Present PHR system

The present system is shown in Fig.1 which is used to store the patient's record. Hospital give raw data to third parties for processing and these third parties generate reports. Even transfer of data is not secure so data can be theft in between during transfer also. Patient should have full control over his own records. It is plainly silly that patient can't have only access to their records just like they would access their bank accounts. And it's good that patients able to see their records at any time without any condition. Present system is not efficient and good for use for storing records. There is big issue of safety, because its social network for every citizen should register and generate their PHR. But this system keeps all the records using cloud. Security is provided to the data by using algorithms. [3],[5]

5] Proposed System:

5.1 System architecture

Design is done according to, the modules needed for the system. Complete System can be ex-plain in two architectural diagrams. First diagram explain flow of patient data to cloud through our system. Second explain retrieving of data on basis of ABE and generation of report.

5.1.1 Architecture diagram part 1(Patient side approach)

This is the proposed system for generating or storing personal health records of patients. The proposed system is divided into five modules for better understanding. Architecture diagram have two approaches and this is architecture diagram is for patient side approach.

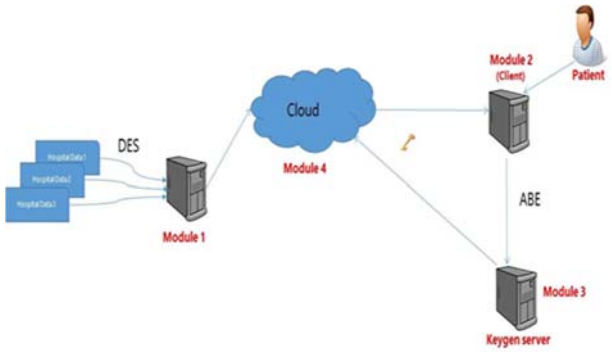

Fig 2: Flow of Patient Data to Cloud

In Fig.2 the initial flow of Patient Data to Cloud is described, in which all the hospitals sends their raw data in a encrypted form to the module 1 of system. In the system module 1 collects this data and arranged in proper manner. Raw data is the collection of patient's records in block of data. At this level partial level of encryption is done with using DES (Data Encryption Standard). At module 1 the data is decrypted and it stores in cloud. When patient wants their record then he can fetch data from cloud and creation of keys is done in key-generator server with using attributes which had given by patient. After that system generates a PHR report that can be viewed by Patient itself or he a give the authority of access to others.

Module 1: This module will get raw data from Hospital trusted servers in encrypted mode and load it into cloud. We will call it raw data Loader.
Module 2: Also called client module. Here patient can access his reports. From client module patient will define attribute set and group policy for encryption. Also PHR encryption will do by taking Master key from Keygen Server or module 3.
Module 3: This server will handle all main tasks like Encryption, decryption, creating policy tree, managing public Keys, Generating Master Key.
Module 4: This module will be cloud where we will store reports and data.

5.1.2 Architecture diagram part 2(Doctor side approach)

This is the proposed system for doctor side approach. The proposed system is divided into five modules for better understanding. Architecture diagram have two approaches and this is second part of architecture diagram is for Data retrieval and report generation.

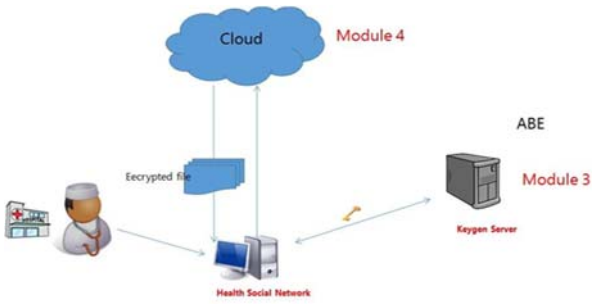

Fig 3: Data retrieval and report generation.

After giving access to a doctor or whom he want to give access generation of report using attribute is done accordingly. A doctor can view the report only if all attributes are matched. Here the main role of Keygen server. The cipher text is related with an access policy over attributes. A user secret key is related with a set of attributes. If the access policy of cipher text and attribute set of secrete key matches then user can decrypt the cipher text.
Module 3: This server will handle all main tasks like Encryption, decryption, creating policy tree, managing public Keys, Generating Master Key.
Module 4: This module will be cloud where we will store reports and data.
Module 5: This module is Health Social Network (HSN) which will be public access for viewing, editing and deleting reports with authorized permission from patient.

6. ALGORITHMS

6.1 ABE algorithm

ƛ- security parameter provided by patient.
G- collection of all identity or attributes.
U- universe description (collection of all identity or attributes user specified).
M- Message (Report).
S Set of attribute provided by user.
Ä- Set of identity provided by receiver.
RD- Raw Data provided by hospital.
PK- public key generated by ABE algorithm.
MK- Master Key generated by ABE algorithm and Access tree (T).
CT- encrypted Report.
SK-private key generated by Key Generator.
M-Decrypted report.
T- Access tree.

1. Setup (ƛ, U) →(PK, MK). The setup algorithm takes as input a security parameter ƛ and universe description U, which defines the set of allowed attribute in the system. It output the public parameter PK and masters secret key MK.

2. Encrypt (PK, M, S) → CT. The encryption algorithm takes as input the public parameters PK a message M and a set of attribute S and output a cipher text CT associated with the attribute set.

3. Keygen (MK, Ä) → SK. This method gives private key SK as output. The key Generation algorithm takes as input the master secret key and an access structure Ä and output a private key SK associated with the attribute.

4. Decrypt (SK, CT) → M. The decryption algorithm takes as input a private key SK associated with access structure A and a cipher text CT associated with attribute set S and outputs a message if S satisfies or the error message ┘ otherwise. The correctness property requires that for all sufficiently large ƛ ε N, all universe descriptions U, all (PK, MK) ε Setup (ƛ, U), all S is subset of U, all SK ε KeyGen (MK, Ä), all M ε M, all A ε G and all CT ε Encrypt (PK, M, S), if S satisfies A, then Decrypt (SK, CT) outputs M.

7. Future Enhancement

Hospitals uses third party services for managing PHR records of patients. Present system is not secure and a big threat to patients personal data. Proposed system provides unique security which will be based on attribute based encryption. So it is completely depends on patient that with whom he want to

share his personal health information. Our system will encrypt report accordingly and make sure that only authorized person can see that report. Any hospital can install our system and provide this functionality to their patients without using any third party services. All data storage will be into cloud so there will be no extra setup cost for database servers. Also because of cloud scalability of system can be easily managed. The main concern is about the privacy of patient personal health data and who could gain access to medical record when they are stored in a cloud server. The data owner and cloud servers are in two different domains in cloud computing storage.

On one hand, cloud servers are not entitled to access the outsourced data contents for data confidentiality on other hand, the data recourses are not physically under the full control of data owner. Storing personal medical records on the cloud server leads to need of encryption mechanism to protect the medical health records, before outsourcing to the cloud. To deal with this the potential risks of privacy exposure, instead of letting the service provides encrypt patients data, medical records sharing services should patient's full control over the selective sharing of their own medical data. To this end, the medical records should be encrypted in addition to traditional access control mechanisms provide by the server. Even in case of failure of one node other cloud node can provide data security. There is big issue of safety, because its social network for every citizen should register and generate their PHR. But this system keeps all the records using cloud.

9. Advantages of Proposed System

Attribute based encryption is used for secure sharing of report.

Patient has Full control over his PHR.

This system has scalable database because cloud is use in this system.

Data availability, Data will be present in different cloud replicas at any point of time. So even in case of failure of one node other cloud node can provide data.

Data security, all data is encrypted using DES algorithm before transferring to another server or machine. In cloud data is stored in unknown multiple servers (Called nodes), so it's hard to hack data from cloud.

There is no third party service. This will not be any third party services.

This system can be installed where patient's data is generated. This system will take data and store it in cloud. That's why there is no third party.

Conclusion

This system is fully patient-centric concept. Patients have full control of its privacy through encrypting their PHR files to allow particular access to other.

The system we has develop is able to cater both statistical reports and ad-hoc reporting in the client- server platform as well as web based platform.Because of cloud Data availability ,Data security is more .This system has scalable database as we are using cloud. We will focus on redesigning the model using keys security, time dimension, database fine tuning to improve on performance and ability to cater for more patient data.

References

1. Ming Li and Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption" IEEE JANUARY 2013.
2. Bharti Ratan Madnani, Sreedevi in Interna-tional Journal of Innovative Research in Computer and Communication Engineering " Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation" white paper MAY 2013.
3. Stiffy Sunny and L. Agilandeeswari in International Journal of Applied Engineering Research, "Secure Data Sharing of Patient Record in Cloud Environment using Attribute Based Encryption" JUNE 2013
4. Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption," master's thesis, Worcester Polytechnic Inst, DEC 2011.
5. J.Hur and D.K.Noh, "Attribute-Based Access Control with efficient Revocation in Data Outsourcning system, "IEEE Trans.Parallel and Distributed system, July2011.
6. S. Narayan, M. Gagne, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW ',JUNE 2010.
7. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, DEC 2010.
8. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in IEEE IN FOCOM'10, MAY 2010.
9. M. Chase and S.S. Chow,"Improving privacy and security in multi-authority attribute-based encryption." in CCS, MAY 2009.
10. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical record-s," in CCSW '09, JUNE 2009.

Biographies

Miss.Ghodake Shubhangi
S.K.N.C.O.E.PUNE,Dept Of computer Engineering.
Email:ghodkeshubhangi12@gmail.com

Miss.Khobragade Pranjali
S.K.N.C.O.E.PUNE,Dept Of computer Engineering
Email:khobragadepranjali@gmail.com

Miss.Joshi Priyanka
S.K.N.C.O.E.PUNE,Dept Of computer Engineering.
Email:priyanka_29joshi@yahoo.com

Miss.Chandak Manjiri
S.K.N.C.O.E.PUNE,Dept Of computer Engineering.
Email:manjirichandak0601@gmail.com.