IJRRECS/June 2014/Volume-2/Issue-6/2489-2496 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

PROTECTING PERSONAL ELECTRONIC HEALTH REPORTS (PEHR) USING HETEROGENEOUS ATTRIBUTE SET ENCRYPTION IN CLOUD SYSTEM

K.V.L.Prabhavathi[1], B.Vijayakumar[2]

[1]M.Tech Student, Dept of CSE, St.Martin's Engineering College, Kompally, Hyderabad, A.P, India

[2]Professor, Dept of CSE, St.Martin's Engineering College, Kompally, Hyderabad, A.P, India

ABSTRACT:

Health Reports are mostly requested to be protected as efficient as they can be protected and accessed only by wanted members. Personal Electronic Health Reports (PEHR) is an patient health model for health information exchange stored at third party like cloud. Because of this, PEHR can be accessed from any place throughout the world. Indeed many encryption logics like Attribute Based Encryption came out for providing security for health reports. Issues such as privacy concerns, managing issues of the health report uploaded, flexible access and remained few issues. In this paper we propose system for different data access control based on role to PEHRs stored in semi-trusted servers. The proposed scheme is an EXTENSION of Attribute Based Encryption algorithm i.e. HETEROGENEOUS ATTRIBUTE SET ENCRYPTION (HASE) with covering of drawback in it. This algorithm generates the key with different attributes of patient report, along with patient details and few heterogeneous attributes is taken as a base to generate the key to avoid problems of Key-Policy attribute encryption. User revocation is also done efficiently by delegating the updates on the uploaded data, providing emergency-key access. HASE not only supports compound attributes due to flexible attribute set combinations. It also also achieves efficient user of multiple role assignments of attributes.

Keywords: Heterogeneous Attribute Set Encryption (HASE), Personal Electronic Health Report (PEHR), Cloud Computing, Efficient access control.

1. INTRODUCTION:

Patient health reports information exchange is model for the sharing of medical records, which allows patient to manage reports efficiently by managing , creating and control person medical information in centralized place through the web or cloud. Patient can now share his/her health reports effectively with a wide range of users such as family members and doctors. Health Service providers are interested to keep their data and application services into the cloud. Cloud computing holds the promise of providing computing:

• The great benefits brought by cloud computing came popular in software industries, academic researchers, and potential cloud users.

• Security in cloud computing in Internet based data storage.

The proposed scheme is an EXTENSION of Single Attribute Encryption [1] i.e. Heterogeneous Attribute Set Encryption(HASE) generates the key with different attributes of patient report , along with patient details and few heterogeneous attributes is taken as a base to generate the key to avoid problems of [2] Key-Policy ABE. Heterogeneous data is taken in all aspects and protects the health report of the user. The traditional method of encrypting data has another drawback that data can be shared only at the level of coarse-grained [6] and so we came up with Attribute Based Encryption. In Attribute Based Encryption a sender can encrypt a message specifying an attribute set and a number N, such that only a recipient with at least N of the given attributes can decrypt the message [7]. Two types of Attribute Based Encryption : Key policy and Cipher text policy have their own drawback to provide more secured encryption.

To handle the key managing part, the users in the system are conceptually divided into two types of domains labeled as public and personal domains[1].

In this paper, we study the patient health report framework, secure sharing of PEHRs stored on semi-trusted third party, and resolves the difficulties of key maintenance issues in different manner, removing drawbacks in [1]. As in previous papers in this paper also we divide Users in two types of domains PUBLIC and PERSONAL domains. We provide analysis of complexity and scalable of our proposed secure PEHR sharing solution.

This paper is compared with several previous papers in complexity, scalability and security and efficient fast processing.

Advantages Provided by HASE:

(1) Security level increases due to double path encryption using different attributes and so the name as Heterogeneous Attribute Set Encryption (HASE) and in this paper we mainly discuss on Heterogeneous attribute set. (2) Modifications on Health Report uploaded by owner can have fine managing on the file uploaded i.e. operations such as upload, modify and delete of the file. (3) Providing efficient key maintenance with typical modules with better performance.

2. PROPOSED SYSTEM FRAMEWORK FOR EFFICIENT PROTECTED 'PEHR'

We consider a PEHR system with multiple PEHR owners and PEHR users. The owners have full control over their PEHR data, i.e., they can do different managing , creating and controlling of files. Distributed server belonging to the PEHR service provider that stores all the owners' PEHRs. The user can be a researcher or relative. While going for cloud computing storage, the report file owner and cloud are in two different domains.

On one hand, servers of cloud are not entitled to access the outsourced data content for data confidentiality. On the other hand, the data resources are not under full control of health report owner. To handle privacy exposure, instead of letting the third party providers encrypt patients data, health reports sharing services should give patients (patient report owners) full control over the selective sharing of their own health report data.

3. REQUIREMENTS TO ACHIEVE PROTECTED 'PEHR' SYSTEM:

To achieve PEHR sharing, the main requirement is:

• Data confidentiality: Unauthorized users without correct privileges will be prevented from decrypting a PEHR document.

• Health report attributes with patient details: To achieve HASE the attributes of patient details is needed along with health report file details for better key maintenance.

• Efficiency and usability: Personal and public domain both are supported by PEHR. Since from public domain it may contain

large size. The health system should be highly flexible in terms of performing key maintenance.

Notations Used For HASE Algorithm:

$\mathcal{U}_D, \mathcal{U}_R$	The attribute universes for data and roles
MK, PK	Master key and public key in ABE
SK	A user's secret key in ABE
P	A key-policy assigned to a user
f	Function applied on key generated

4. OVERVIEW OF PROPOSED FRAMEWORK VIEW:

Framework Flow:

In our framework, multiple Attribute Authority (AAs), and multiple users in multiple domains. Fig1 divides the system into multiple domains as Public and Personal domains according to the different user's data access requirements. In different domains, we utilize HASE to realize key for PEHR access. Especially, in a Public domain multi-authority HASE is used. Each data owner is a trusted authority of her own Personal domain.

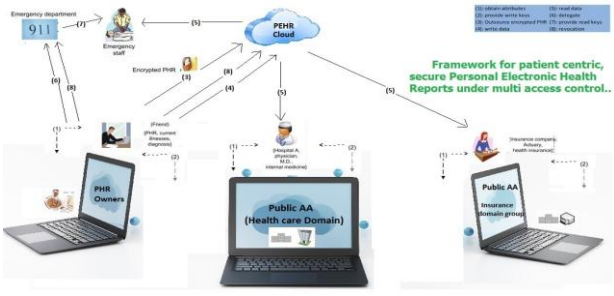

Fig.1 High-level Overview of Framework.

Heterogeneous Attribute Set hierarchy of Health Report files: Fig 2: Different Attributes used for encrypting and stored in Cloud Storage. Universal attributes such as "medical history", "Examination", "and diseases like allergies". Each PEHR owner's client application generates its corresponding master keys. The master keys can be published combination of both the secret and public keys.

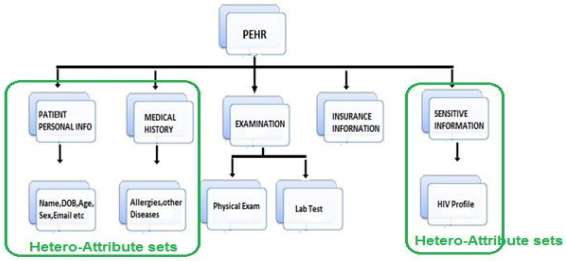

Fig. 2: Heterogeneous Attribute Hierarchy Set of health report files.

System Flow: User through web application will login into the system. The user credentials will be checked against cloud. System will verify that to which domain user is linked. On that basis attribute authentication system will grant different read/ write access. If user wants to write

some data to PEHR cloud than application server will encrypt that data with HASE and then it will be stored in PEHR cloud. Key distribution will be again managed by application logic server.

5. HASE ALGORITHM AND IMPLEMENTATION

Algorithm:

In particular, the Attribute Authority first generates the **SK** and **PK**. Typical access policies in this algorithm is expressed with AND, OR operations by assigning unique id for each user in the proposed system. '*P'* is applied with the combination of AND , OR operations

f(MK) = f(SK) + f(PK)

f(SK) – Can be a attribute like Health Report File Name that is secret and apply function on the respective attribute.

f(PK) – Can be a attribute from public keys like Owner Name and apply function on the respective attribute. Combination of u_d and u_rf(MK) – The function of final master key formed by combining secret and primary key and passing with the data to encrypt the data at user level and store in semi-trusted third party cloud. In this algorithm the function used is converting string to byte.

IMPLEMENTATION Modules:

The operations of proposed health report sharing system combine HASE and traditional cryptography, allowing patients to share their health reports. These operations can be classified into following modules:

Modules of the system are:

1. Key Generation
2. Encryption of Patient Health Reports. HASE Encryption.
3. View Health Reports (Decryption).
4. Managing Reports by Owner.
5. Identity Based Support for Key through E-Mail

1. Key Generation:

In key generation we follow two keys generation. One is the Secret Key and the

other is Public Key generation. Together form a Master Key generation for efficient and fast key maintenance protection of Patient Electronic Health Reports (PEHR) system.

Secret key: This key is generated by encrypting the file name in stream. This is one sample attribute that can be taken for Secret key generation. Based on the secret key masker key later the data is decrypted.

Public Key: This key is generated by encrypting the user details in the stream. Public key is mostly concentrated on user details. Public Key is generated from the many or one attribute of the user. These attributes place crucial role in generating key.

Master Key: As show in below Fig 4, the Master key is created i.e., combined the Secret and Public Key.

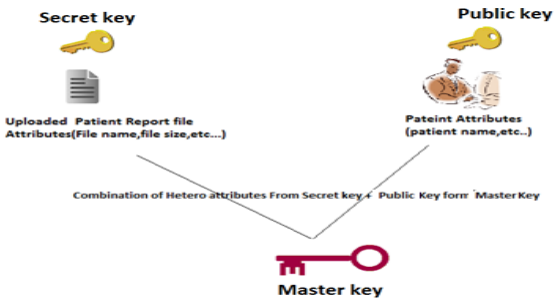

Fig. 4: Key Generation module of HASE in PEHR system.

2. Encryption of Patient Health Reports. HASE Encryption:

The Patient Encrypt the electronic health reports under a role-based access policy in Public domain for write access, and under a selected set of attributes that provides access for different users in personal. The Key along with Data is encrypted and Uploads Encrypted File to the cloud server. Fig 5 below shows the Flow Diagram for the encryption.

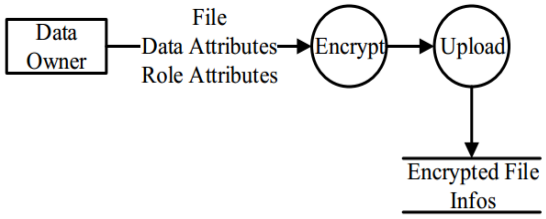

Fig 5 – Data Flow Diagram for Encryption and Upload

3. View Health Reports (Decryption):

View Medical Record File /Decryption: User from the personal or public domain can request the file form the server. Based

on the role of the person the access is provided as show in fig 1. Only user can view the records, provided the key policy matches with the attributes attached with the files.

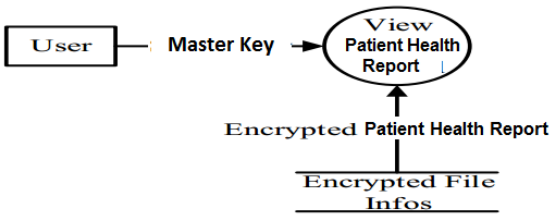

Fig 6 – Dataflow Diagram for the Decryption

4. Managing Health Reports by Owner:

The Owner of the Health Reports Once uploaded can also have chance to modify the uploaded file, delete or perform operations on the Health Report. This flexibility is provided for the owner for efficient managing of Health Reports.

5. Identity Based Support for Key:

As a process of HASE the attributes are gathered in all the ways and encrypted and then stored in cloud. The Key generated is send as *E-mail* to the respective member's i.e., to the respective domain members with defined access control. Adding to this proposed paper security access is defined based on the role. Even the entered key is same for different roles and same master key is send as email, based on the role the access is provided. Permissions to generate keys can be controlled dynamically in real time.

6. CONCLUSION

In this paper, the propose frame work of EXTENSION of Attribute Based Encryption with HASE for PEHR system with secure sharing health reports. Considering semi- trustworthy cloud servers, we discuss that patients have complete control of their own privacy by encrypting their PEHR files to efficient role access. Providing efficient management of the health report uploaded. The framework highlights the challenges brought by multiple PEHR owners and users, by reducing the complexity of key managing with guaranty. HASE is used to encrypt the PEHR allow access by personal users, and also various users from different domains. Adding to HASE providing Identity Based Encryption by sending email is the better way to provide the authentication for the Personal Health Reports System.

As an extension of this paper a web-service can be provide to access the same encrypted data that is presented in the cloud so that the cloud data can be accessed from

different applications like mobile or any type of application by owner. As a security, the layer of firewall can also be provided in web-service and adding alerts on health report view.

REFERENCES

[1] Ming Li., Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou" Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,vol.xx,No.xx,2012

[2] H. Lohr, 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] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06),pp. 89-98, 2006.

[4] Angelo De Caro and Vincenzo Iovino, "jPBC: Java Pairing Based Cryptography" Computers and Communications (ISCC), 2011 IEEE Symposium on Digital Object Identifier: 10.1109/ISCC.2011.5983948 Publication Year: 2011 , Page(s): 850 – 855

[6] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlledencryption: ensuring privacy of electronic medical records,"in CCSW '09, 2009, pp. 103–114.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for .ne-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98.

[8] Dr.V.L.Jyothi2, Professor & Head, Department of CSE, Jeppiaar Engineering College, Chennai-119.National Conference on Architecture, Software systems and Green computing-2013(NCASG2013) ISBN NO: 978-93-80609-14-0, Jan , 2013

[9] J. Bethencourt, A. Sahai, and B. Waters,"Ciphertext-policy attribute-based encryption," in IEEE S& P '07, 2007, pp. 321–334.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98.

[12] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEEWireless Communications Magazine, Feb. 2010.