Review on Encryption Techniques of Personal Health Records in Cloud Computing

[1]Anparasi K, [2]ShanthaVisalakshi U
[1]Research Scholar, [2]Assistant Professor
Ethiraj College for Women,Chennai

Abstract **- Personal health record (PHR) is an emerging trend in the health field for the exchange and use of personal health information. The PHR is stored in third party, such as cloud providers. Cloud Computing system is one of the rapidly growing computing technology's distributed model. Even though technology is growing rapidly, there are many security problems related with the storage of personal health information in the cloud system, which induces numerous security challenges to the PHR privacy and confidentiality. There are different types of approaches are used to protect the privacy of this system. In this paper, some encryption techniques such as Attribute Based Encryption (ABE), Cipher text Policy-Attribute Based Encryption (CP-ABE), Key Policy-Attribute Based Encryption (KP-ABE), and Multi-Authority Attribute Based Encryption (MA-ABE) are discussed. This paper also discusses about how the above mentioned techniques contribute in securing the PHR in cloud system.**

Index Terms **- Cloud Computing, PHR, Attribute Based Encryption (ABE).**

I. INTRODUCTION

The most widely used regulations are the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the European Data Protection Directive 95/46/EC. Cloud computing is an efficient technique by the user can access any data from anywhere anytime through internet. The Personal Health Records (PHR) is thus also using this cloud computing technology for the efficient storage and retrieval system. In PHR, a patient can create, manage and control their personal health data in one place such as data center through the internet.

The PHR data should secured from the external and internal attackers. When the PHR owner upload the PHR data to the cloud server, the owner is losing the physical control over the data and make lots of security challenges to the PHR privacy and confidentiality. To ensure privacy control over the owner's own PHRs, the fine-grained data access control mechanism is essential.

For more secure and effective storing, the Attribute Based Encryption (ABE) is used. It is also used for retrieving and sharing the data in PHR. But in ABE, the user revocation is again the challenging problem in PHR. So, to overcome this revocation problem, the Cipher text Policy-Attribute Based Encryption (CP-ABE) and Key Policy-Attribute Based Encryption (KP-ABE) are also used. In PHR, there are number of owners and users can access the data. To providing multiple keys or attributes in PHR, the Multi-Authority Attribute Based Encryption (MA-ABE) is used.

II. SYSTEM ARCHITECTURE

This system is given that the fine-grained access to the system by using the different attribute based encryption techniques.The users of this system are classified into two security domains such as Personal Domain (PSD)includes family members, friends. Public Domain (PUD)includes doctors, nurses, medical researchers, health care organization and insurance field.

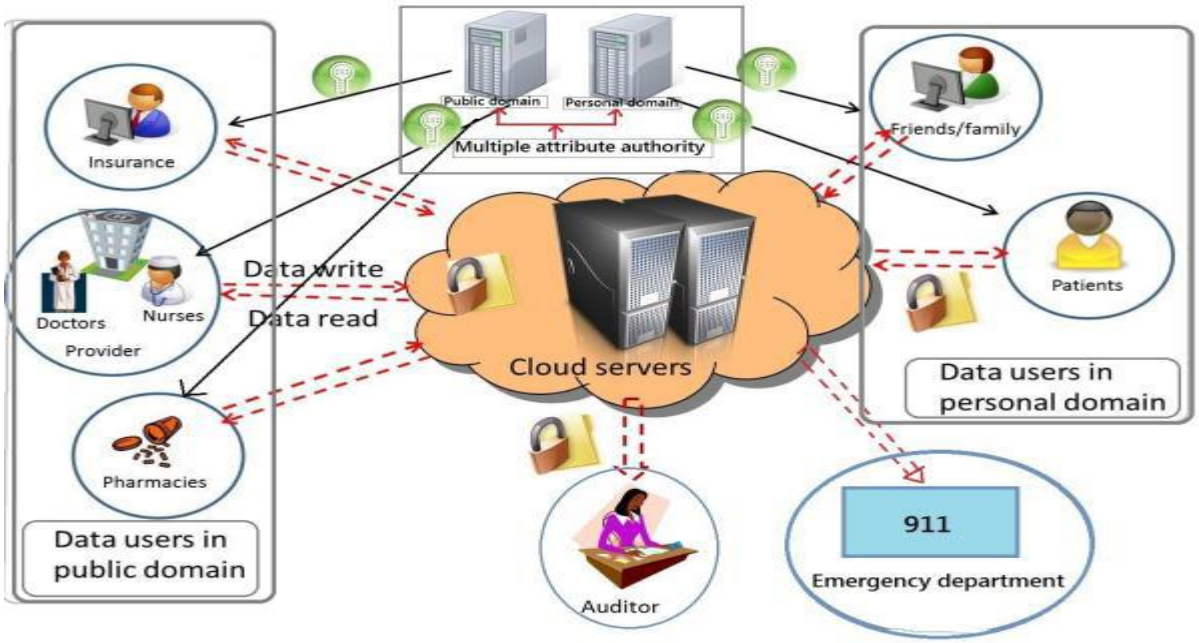

Fig1:-System Architecture

In this architecture PUD uses multi-authority ABE which there are multiple Attribute Authorities (AAs), each authorities have their own attribute value. Many attribute based encryption are used for the above mentioned domains. Key-policy attribute based encryption technique is used.

III. ATTRIBUTE BASED ENCRYPTION

The ABE provides the security to the database. The authority, data owner and data user are the main entities in this system. To generate the keys for data owners and users is the role of authority. The authority generate the keys based on the attributes such as public key and private key. The user who have a minimum number of attributes only can decrypt the data. So while using this method the owner need not to know about the entire list of users instead of that they can encrypt the data according to some attributes only. If any data user wants to add their medical information to this system and he owns to attributes not include pre-defined attributes.

The authority can re-define attributes and generate a public key and master key again. To encrypt the data with a public key and a set of descriptive attributes is the role of data owner. To decrypt encrypted data with his private key sent from the authority and then he can obtain the needed data is the role of data user.For decrypting the data, attributes in data user's private key will check by matching with attributes in encrypted data. If the number of matching is a threshold value ***d***, the data user's private key will be permitted to decrypt the encrypted data.

IV. CIPHER TEXT POLICY-ATTRIBUTE BASED ENCRYPTION

CP-ABE is an attribute based encryption technique which, allow the data owner to encrypt the data based on an access policy. The decryption is possible when the secret key is matching with the access control policy. The basic idea of CP-ABE is the user secret key is associated with a set of attributes and each cipher text will embedded with an access structure. The user can decrypt the message only if the user's attribute satisfied with the access structure of the ciphertext.

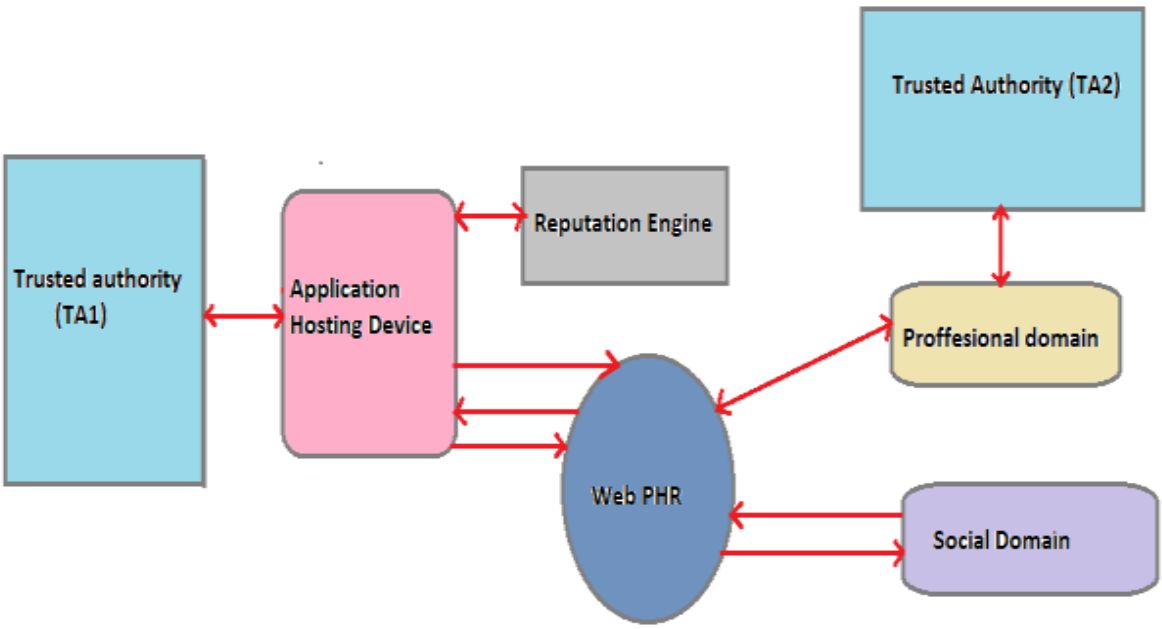

Fig2:- PHR System

In this system, for the purpose of attribute issue there are two trusted authorities Trusted Authority1 (TA1) for the professional domain and Trusted Authority2 (TA2) for the social domain are used. Here, the patient can act as this second trusted authority (TA2). Security key are generated for the users of the social domain.

The Cipher text Policy-Attribute Based Encryption technique consist four algorithms.

- ***Setup Algorithm (MK, PK)***: This algorithm runs by the trusted authority or the security administrator. It will take input a security key ***k*** and output a master secret key ***MK*** and a master public key ***PK***.
- ***Key Generation Algorithm (SK):*** It also run by the trusted authority and takes input a set of attributes and ***MK***. It has the output a user secret key ***SK*** associated with the attribute set.
- ***Encryption Algorithm (CT):*** It is run by the encryption of the system. It has the input a message m, a master key ***PK*** and an access policy ***P***, the output of the algorithm is a cipher-text ***CT*** under the access policy ***P***.
- ***Decryption Algorithm (m):*** It is run by the description of the system. The input for the algorithm is the cipher-text ***CT*** to be decrypted and the user secret key ***SK***. The output of the algorithm is message ***m***, if and only if the secret key of the user satisfies the access policy ***P***, under which the message was encrypted. It shows an error message if the secret key does not satisfy the access policy ***P.***

V. KEY POLICY-ATTRIBUTE BASED ENCRYPTION

KP-ABE is an attribute based encryption, in which the data are associated with the attributes for each public key component is defined. The ciphertext key can be decrypted by using this technique. The key policy-attribute based encryption and cipher text policy-attribute based encryption technique are almost same in their working scenario. But both are having some difference in terms of specifying the access policy for the users. The KP-ABE is useful for providing the fine-grained access control to the data system where it can efficiently specify that which part of data system can be accessed by which user and what are the operations they can execute over the system. The Key Policy-Attribute Based Encryption technique consists of four algorithms such as *Setup(), KeyGen(), Encrypt()* and *Decrypt().*

VI.MULTI-AUTHORITY ATTRIBUTEBASED ENCRYPTION

The MA-ABE is an advanced attribute based encryption technique and this system consists of *k* attributes and one central authority. Among these *k* attributes, each attribute is assigned a value *dk*. In the PHR system, the users will be from different area like the doctors from hospitals, personal relations and the other users from the insurance field. So each user will have different access control mechanism based on the relation with the patient or owner.Main advantage of MA-ABE provides the scalability to the PHR system. Limitation of this technique is it exposesencrypted access policy.

The Multi-Authority Attribute Based Encryption technique consists of five algorithms:

- ***Set up Algorithm:*** A random algorithm that is run by the central authority or some other trusted authority. It takes the input as security parameter and outputs a public key. The secret key pair for each of the attribute authorities and also outputs a system public key and private secret key which will be used by the central authority.

- ***Attribute Key Generation Algorithm:*** A random algorithm run by an attribute authority. It takes the input is authority's key, the authority's value ***dk*** and a set of attributes in the authority's domain and outputs the secret key for the user.

- ***Central Key Generation Algorithm:*** A randomized algorithm that is run by the central authority. It takes an input as the master secret key and outputs another secret key for the user.

- ***Encryption Algorithm:*** A randomized algorithm runs by a server side sender. It takes the input as a set of attributes for each authority, a message and the system public key and the output is cipher text.

- ***Decryption Algorithm:***A deterministic algorithm runs by a client side user. It takes input as a cipher text and this input is encrypted under attribute set. Outputs of this algorithm are message***m***.

VII. CONCLUSION

In this paper different attribute based encryption techniques that can be used in cloud computing system for security, privacy, flexible, scalable and fine grained access control into the PHR system are discussed. By using appropriate encryption technique, the owners can protect their valuable medical information against the security problem in cloud system. In future, further enhancements of these encryption techniques can provide high security and privacy of PHR.

REFERENCES:

[1] Neetha Xavier and V.Chandrasekar "Security of PHR in Cloud Computing by Using Several Attribute Based Encryption Techniques" International Journal of Communication and Computer Technologies, Volume 01 – No.72 Issue: 07 Nov 2013.
[2] M. Vijayapriya and Dr. A. Malathi "On Demand Security for Personal Health Record in Cloud Computing Using Encryption and Decryption Cryptography" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 9, September 2013.
[3] M. Li, S. Yu,Y. Zheng, ,K. Ren, &W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,IEEE Transactions on Parallel and Distributed Systems,vol. 24(1), pp. 131-143, 2013.
[4] Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption", IEEE Transactions On Parallel And Distributed Systems 2012.
[5] L. Ibraimi, M. Petkovic, S. Nikova, P.Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.
[6] Melissa Chase, "Multi-authority Attribute Based Encryption", TCC, volume 4392 of LNCS, pages 515–534, Springer, 2007.
[7] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal HealthRecords in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'lICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.
[8] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption,"technical report, Univ. of Twente, 2009.
[9] PriyankaKorde, Vijay Panwar and SnehaKalse, "Securing Personal Health Records in Cloud using Attribute Based Encryption,"International Journal of Engineering and Advanced Technology (IJEAT), Issue-4, April 2013.