International Journal of Research in Advent Technology, Special Issue, March 2019
E-ISSN: 2321-9637
International Conference on Technological Emerging Challenges (ICTEC-2019)
Available online at www.ijrat.org

Secure And Searchable Access Control Scheme For Personal Health Record In Cloud Computing

E.V.N.Jyothi[1], B.Rajani[2], Dr.V.Purna Chandra Rao[3].
Ph.D.Scholar[1], Department of Computer Science and Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University,India.
(Assoc. Professor in CSE Dept. in PACEITS)
PhD Scholar[2], Department of Computer Science and Engineering, Shri Jagdishprasad Jhabarmal Tibrewala University,India.
(Assoc. Professor in CSE Dept. in KMIT)
Professor[3], Department of Computer Science and Engineering, SVIT, Hyderabad, India.

Abstract: Cloud computing is one of the most advanced technology in recent years. Since this new computing technology requires users to entrust their data to cloud providers. Personal health record (PHR) is an patient-centric model of health information exchange in which the information are outsourced to be stored at the third party server, called as cloud providers, such that security and privacy of the outsourced data should be preserved. The need for secure storage, communication and efficient key management renders the approach impractical. The current work focuses on reducing key management overhead by generating a single aggregate key, but does not provide, how it can satisfy the principles of efficient data sharing. So, we propose a scheme to achieve: confidentiality of personal health data, authenticity of personal health data. Here the user type of each user is organized in a hierarchical manner and it represents the hierarchical structure of the users. The patient details are encrypted using Hierarchical Attribute Set Based Encryption technique. Role of one user is encrypted to another user such that scalability, access control and efficient user revocation is achieved and also it proves the security of HASBE based on security of the Cipher text-Policy Attribute-Based Encryption (CP-ABE) scheme and analyze its performance and computational complexity.

Key Words: HASBE, cloud computing, personal health records, fine-grained access control

1. INTRODUCTION

Cloud computing enables users to remotely store their data in a cloud. Moving data from the user side to the cloud provides a great convenience to users, so that user can access data in the cloud anywhere at any time. Especially for small and medium-sized enterprises with limited budgets, they can achieve cost savings and the flexibility to scale investments on-demand, by using cloud-based services to manage projects, enterprise-wide schedules and the contacts. An untrustworthy cloud service provider(CSP) may sell the confidential information about an enterprise to its business person for making a profit. Therefore, to keep the sensitive data confidential the particular data is encrypted and stored in the cloud.

Personal health record (PHR) is an patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. S. Chow et.al[1]have proposed Achieving Secure, Scalable, And Fine-Grained Data Access Control In Cloud Computing enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information. We achieve our design goals by exploiting a novel cryptographic primitive, namely key policy attribute- based encryption (KP-ABE) and uniquely combine it with the technique of proxy re-encryption (PRE) and lazy re- encryption.

To ensure data privacy and access control, PHR owners choose to encrypt their data before uploading it on the cloud and hence the data remains secure against the cloud providers and other malicious users. Suppose that patients want to share their PHRs with different data users, there are two ways to achieve this under traditional encryption scheme:

- Data owner (patient) encrypts all categories of personal health records with a single encryption key (symmetric key cryptosystem) and gives the data users like doctors, nurses the corresponding secret key directly.
- Data owner (patient) encrypts different categories of personal health records with different keys and sends the corresponding secret keys to data users like doctors, nurses, relatives etc.

2. LITERATURE SURVEY

Several recent studies have focused on the issue of secure sharing of electronic health records in the cloud.

Chen *et al.* [4] proposed an EHR solution, relying mainly on smart cards and RSA that enables patients to store their medical records on hybrid clouds. In this approach, patients' medical records are stored in two types of cloud: the hospital's private cloud and the public cloud. The authors discussed two usage cases. The first is that of the medical records being accessed by the owner of the data, *i.e.*, the doctor who created the records. They can directly access the records from their private cloud or from the public cloud. The second case is that of the medical records being accessed by other hospitals, who must seek permission from the data owner before they can access the records. The authors also provide a solution for

emergency situations. However, the shortcoming of this approach is that data owners, *i.e.*, doctors have access control for the medical records and their computing load is heavy.

Leng *et al.* [5] proposed a solution that allows patients to specify a policy to support fine-grained access control. They primarily utilized Conditional Proxy Re-Encryption to enforce sticky policies and provided users with write privileges for PHRs. When users finish writing data to their PHRs, they sign the modified PHRs. However, users sign the PHRs using the signature key of the PHR owner and it is therefore difficult to correctly verify who signed the PHRs.

Kuo et al. [2] proposed a scheme for patient-centric access control over PHR data. The proposed scheme ensures the following security properties: (1) confidentiality of health data, (2) integrity of health data, (3) authenticity of health data, (4) patient-centric fine-grained access control, and revocation of access control using symmetric key cryptosystem and proxy re-encryption (PRE) scheme. But the main drawback of this scheme is, each file category is encrypted with distinct secret key so whenever a data user (e.g. Doctor or nurse) wants to update PHR categories, patient have to provide the corresponding secret keys. Besides this, the scheme is based on proxy re-encryption scheme which requires data owners to have too much trust on the proxy that it only converts cipher texts according to his instruction. A PRE scheme allows data owners to delegate to the proxy the ability to convert the cipher texts encrypted under his public key into ones for data users. Hence it is desired that proxy doesn't reside in the storage server. This increases communication overhead since every decryption requires separate interaction with the proxy.

Chu et al.[1] proposed a new public key cryptosystem which can aggregate any set of secret keys to generate a single compact aggregate key encompassing the power of all the keys being aggregated. But the work did not focus on how it can help patients to have fine grained access control and revocation of access control and at the same time ensuring confidentiality, authentication and integrity of their PHRs.

So in this paper, we redesign the scheme in [2] for patient-centric access control over PHR data belonging to the patient using the concept of a key-aggregate cryptosystem. Our solution ensures the following security properties: (1) confidentiality of personal health data, (2) integrity of personal health data, (3) authenticity of personal health data, (4) patient-centric fine-grained access control, and revocation of access control.

3. PROPOSED SYSTEM

3.1 User Interface Design

The goal of user interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goal. Good user interface design facilitates to completing the task. Graphic design may be utilized to support its usability. The design process must balance technical functionality and visual elements to create a system that is not only operational but also usable and adaptable to changing user needs.

3.2 Cloud Provider

A service provider offers customers storage or software services available through cloud. Services made available to users on demand in which cloud provider's provide a service in on demand to the data owners. The cloud service provider manages a cloud to provide data storage service in which data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner.

3.3 Access Control Policy For PHR Data

In the architecture of the proposed scheme, PHR data are divided into different categories and arranged in hierarchy as shown in Fig 1. PHR data may include several medical records like dental records, medical records and other categories like personal information, insurance policy information etc.

PHR owners specify policies for their PHR data to grant access privileges to each user. A policy may contain the following details:

(1) Role: users who are permitted to access the data, for example, the doctor, nurse, or insurance broker.
(2) Category of PHR data: Personal Information, Laboratory Test Reports, Medical History, etc.
(3) Permission: includes read, write, and even print.

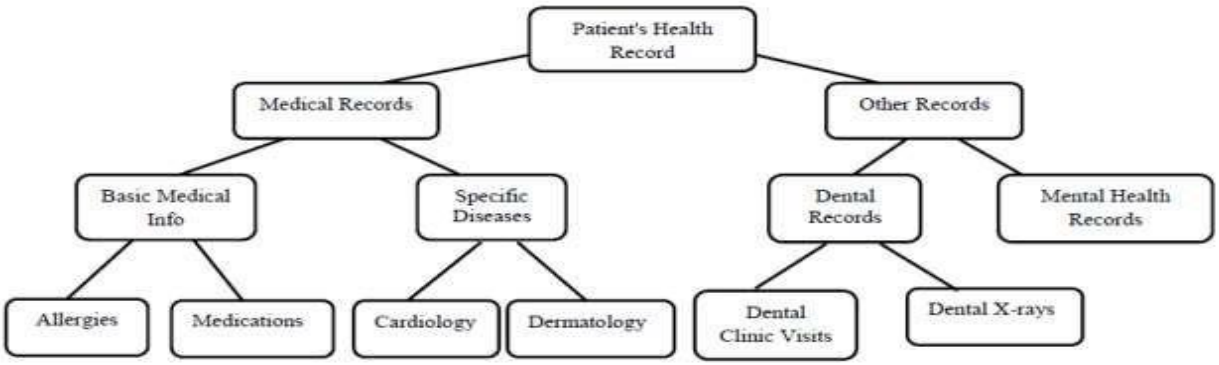

Figure 1. A hierarchical personal health record

3.4 Key Generation (pk, msk):

This algorithm is executed by the patient to randomly generate a public/master-secret key pair (pk, msk).

3.5 Encrypt (pk, i, d):

This algorithm is executed by anyone who wants to encrypt data. On input a public-key pk, an index i denoting the PHR category, and a document d, it outputs a ciphertext C.

3.6 Extract (msk, r, S):

This algorithm is executed by the patient for delegating the decrypting power for a certain set of ciphertext classes to a delegatee. On providing input of the master secret key msk, an access right r and a set S of indices corresponding to different classes, it outputs the aggregate key for set S denoted by KS.

3.7 Decrypt (KS, S, i, C):

This algorithm is executed by a data user who received an aggregate key KS generated by Extract. On input KS, the set S, an index i denoting the file category the ciphertext C belongs to, and C, it outputs the decrypted result, if C □ S.

4. SOLUTION ANALYSIS

A. Confidentiality of Personal Health Data:

Before uploading a health record i, it is encrypted using the product of $(pk)_i$ and $(msk)i$. The master secret key is kept secret. When patient generates an aggregate key which is the product of master secret keys, data user or an interceptor cannot obtain each multiplier from the product. Hence, even pk_i component of the encryption key is publicly available, other component msk_i is hidden hence confidentiality of personal health data is ensured.

B. Authenticity of Personal Health Data:

In our proposed scheme owner of the PHR generates an aggregate key. At the time of decryption,an aggregate key successfully decrypts the authorized set of cipher text. This verifies the authenticity of personal health data.

C. Patient-Centric Fine-Grained Access Control:

In our scheme, the PHR owner generates a value representing a particular access right when generating the aggregate key. The PHR owner can therefore control access privileges for every user.

D. Revocation Of Access Control:

If the PHR owner wishes to revoke some users in a certain category, then they need only to replace the aggregate key K_s with K_{s1}. The small aggregate key size minimizes the communication overhead for transferring the new key. Revocation therefore, is easily achieved.

5. DISCUSSION ON RESULTS

Personal Health Record contains personal information in which the cloud providers used to provide the service for the users to share personal information.

By sharing of information each user type can only have the permission to access their record. The proposed system using HASBE ensures the scalability and efficiency of sharing only the encrypted data with the users. The parameters are discussed as,

1) Efficiency

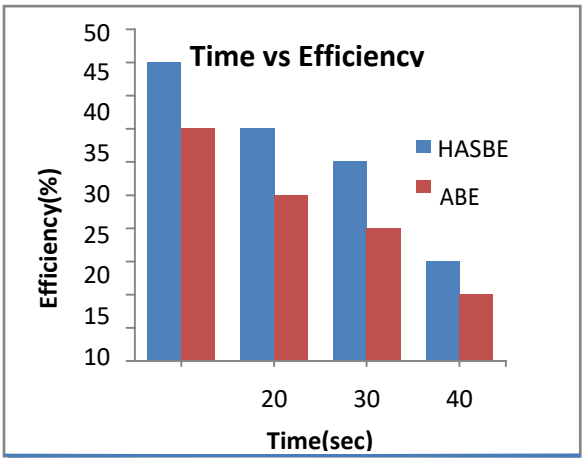

Figure 2.Efficiency of PHR

The figure 2.shows that efficiency is increased in the propsed system using HASBE, because sharing of information is encrypted and each user type can access the information with their privilages provided by the cloud providers,so that the performance of HASBE is increased compared to the existing system of ABE .

2) Scalability

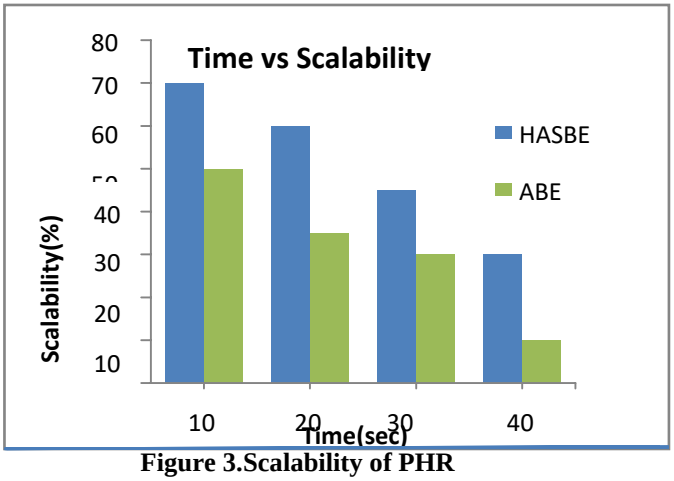

Figure 3.Scalability of PHR

The figure 3.shows that scalability is increased in the proposed system using HASBE, The domain and trusted authority is used because of using the trusted authority, the delegating key is maintained. So that the user can share a information in a scalable manner.

6. CONCLUSION

With the increasing popularity of modern healthcare systems based on cloud storage, how to protect PHRs stored in the cloud is a central question. Cryptographic techniques are getting more versatile and often involve multiple keys for a single application which increases the key management overhead. In this paper, the issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, has been analyzed. The proposed framework of secure sharing of personal health records in cloud computing, considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations.

REFERENCES

[1] C. Chu, S. Chow, and W. Tzeng, “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems, 2014, 25 (2): 468- 477.
[2] Kuo-Hsuan Huang, En-Chi Chang, and Shao-Jui

Wang, "A Patient-Centric Access Control Scheme for Personal Health Records in the Cloud", Fourth International Conference on Networking and Distributed Computing, 2014.

[3] Dixit, G. N. "Patient Centric Frame Work For Data Access Control Using Key Management In Cloud Server", International Journal of Engineering, *2* (4), 2013.

[4] Chen, Y. Y., Lu, J. C., & Jan, J. K. "A secure EHR system based on hybrid clouds," Journal of medical systems, 36 (5), 3375- 3384, 2012.

[5] Leng, C., Yu, H., Wang, J., & Huang, J. "Securing Personal Health Records in the Cloud by Enforcing Sticky Policies," TELKOMNIKA Indonesian Journal of Electrical Engineering, 11 (4), 2200-2208, 2013.

[6] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records", Proc. ACM Workshop Cloud Computing Security (CCSW 09), pp. 103-114, 2009.

[7] Chen Danwei, Chen Linling, Fan Xiaowei, He Liwen, Pan Su, and Hu Ruoxiang "Securing Patient-Centric Personal Health Records Sharing System in Cloud Computing", China Communications, Supplement No.1, 2014.

[8] Ming Li, Shucheng Yu, and Yao Zheng, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE Transactions on Parallel and Distributed Systems, 24(1), pp. 131-143, 2013.

[9] 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.

[10] M. Chase, and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009.

[11] R. Canetti, and S. Hohenberger, "Chosen-Ciphertext Secure Proxy Re- Encryption", Proc. 14th ACM Conf. Computer and Comm.Security (CCS 07), pp. 185-194, 2007.

[12] S.S.M. Chow, J. Weng, Y. Yang, and R.H. Deng, "Efficient Unidirectional Proxy Re-encryption", Proc. Progress in Cryptology AFRICACRYPT, vol. 6055, pp. 316-332, 2010.

[13] Mell, Timothy Grance, "The NIST Definition of Cloud Computing", NIST Special Publication 800-1145, Sept. 2011.