IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. VII (Mar-Apr. 2014), PP 70-74
www.iosrjournals.org

Secure Personal Health Records access in Cloud Computing

R.Shreelakshmi [1], S. Pandiyarajan M.E [2], Dr. J.Jagadeesan[3]
[1] *M.Tech Student, Department of Computer Science and Engineering, SRM University, India*
[2] *Assistant Professor, Department of Computer Science and Engineering, SRM University, India*
[3] *Head of Department, Department of Computer Science and Engineering, SRM University, India*

Abstract: *Patient Health Record (PHR) is a complete Patient related health data, which is getting stored in cloud computing to gain cost benefit and better access control. In maintaining PHR, cloud computing plays an inevitable role, since small hospitals and physicians are not affordable to maintain own servers to keep PHRs for cost and security reasons . Providing accessibility to variable stake holders like Patients, Physicians, Hospitals and Insurance Providers, become a tedious process in private individual servers with encryption mechanisms. Cloud solution ensures that PHRs ' availability to the necessary stake holders at any point of time. In any country , there are laws which governs to maintain privacy of patient health records, and hence maintaining PHRs in cloud are subjected to privacy concerns and high risk of getting exploited. There are various encryption schemes exist to preserve PHR's security and privacy in Cloud computing. In this paper, we propose a secure PHR accessing scheme for dynamic environment to preserve privacy in semi trusted cloud servers .*

Keywords: *Personal Health Record, Cloud computing, dynamic group, secure access control*

I. Introduction

Patient Health Record (PHR) is nothing but a patient health information which could be a complete data that is related to patient starting from Blood group, Lab reports to scan images. PHRs are also termed as EHR (Electronic Health Record) and EMR (Electronic Medical Record) are stored in cloud servers' storage in order to utilize high quality infrastructure with cost benefit.

In general practice, each patient maintains his/her Personal Health Records for future reference. Hence maintaining them personally is a tedious task. Moreover the PHRs could be shared with many Physicians and Hospitals as and when required. Patient has to carry all the hardcopy documents along with him/her. If the patient has more records, then he/she has to maintain them in order, which warrants more meticulous attitude and practice.

Instead of maintaining physical hard copies of records, patient can maintain those records in the system in electronic format, which could be shared with Physicians, Surgeons, Insurance companies and Third Party Administrators (TPA).

Keeping Patient Health Records in cloud computing is a practical solution for effective storage and easy access. A patient can allow physicians, surgeons, patient's relatives, emergency cell , Insurance companies and TPAs to access the PHRs . By utilizing the cloud, the patient can be completely released from the troublesome local data storage and maintenance.

Keeping PHRs in cloud faces a high risk of maintaining confidentiality and privacy which are two important security aspects of maintaining PHRs. The cloud servers are maintained and managed by cloud service providers, patient cannot trust the cloud with confidence, hence generally cloud environment is known as un trusted environment.

To preserve data privacy, confidentiality and integrity a basic solution is to encrypt PHRs, and then upload the encrypted PHRs into the cloud. Hence designing an efficient and secure PHR access scheme for multiple groups in the cloud is challenging due to the following issues.

1. Patients' real identities could be easily disclosed to cloud service providers and attackers of cloud.
2. There are chances that any criminal minded person in Hospital or Insurance Company or TPA could misuse the PHR in cloud
3. If the patient enables encryption, it will be a tedious job for the patient to change the key as and when members access the PHR vary, since the physician/Insurance company members could be newly added/ moved out of the organization
4. If proper key management is not employed there could be a chance that even the member of a hospital resigns, still he/she could access the PHR from outside which puts PHRs in great risk.

To solve the above challenges mentioned above, we propose, a secure multi-owner PHR accessing scheme for dynamic groups in the cloud.

The main contributions of this paper include:

1. Proposal of secure PHR accessing method to accommodate dynamic groups like hospitals, insurance companies and TPAs to do dynamic sharing of data
2. Proposed method will support user revocation easily without sharing the new secret keys in case any of the existing member leaves the group. This is essential since PHRs access group could become larger and larger

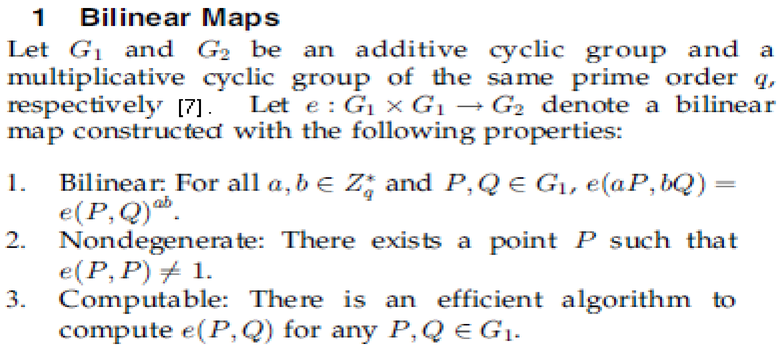
II. Related Work

This paper is mostly related to works in [1] which shares the effective method of data sharing . Also related to works in cryptographically enforced access control for outsourced data and attribute based encryption. To realize fine-grained access control, the traditional public key encryption (PKE)-based schemes [2],[3] either incur high key management overhead, or require encrypting multiple copies of a file using different users' keys. In [4], Kallahalla et al. proposed a cryptographic storage system which enables secure file sharing on un trusted servers, named Plutus. By dividing files into file groups and encrypting each file group with a unique file-block key, the data owner can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation.

In [5], files stored on the un trusted server include two parts: file metadata and file data. The file metadata implies the access control information including a series of encrypted key blocks, each of which is encrypted under the public key of authorized users. Thus, the size of the file metadata is proportional to the number of authorized users.

The user revocation in the scheme is an intractable issue especially for large-scale sharing, since the file metadata needs to be updated. In their extension version, the NNL construction [6] is used for efficient key revocation. However, when a new user joins the group, the private key of each user in an NNL system needs to be recomputed, which may limit the application for dynamic groups. Another concern is that the computation overhead of encryption linearly increases with the sharing scale.

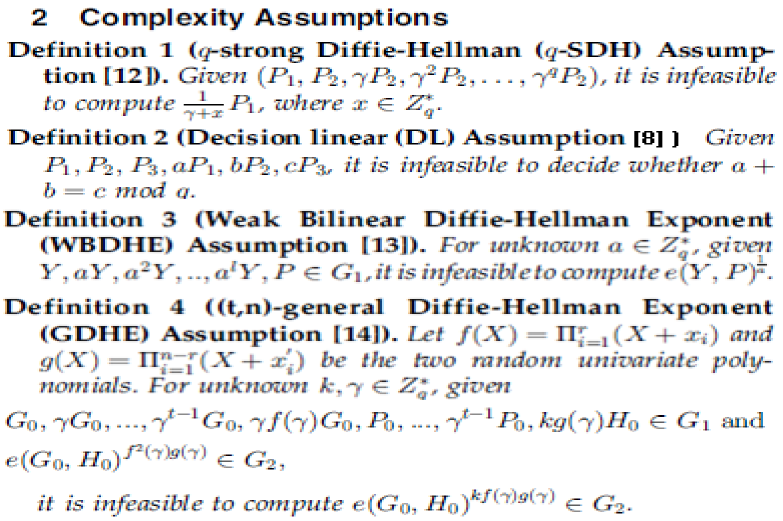
III. Preliminaries



1 Bilinear Maps

Let G_1 and G_2 be an additive cyclic group and a multiplicative cyclic group of the same prime order q, respectively [7]. Let $e : G_1 \times G_1 \rightarrow G_2$ denote a bilinear map constructed with the following properties:

1. Bilinear: For all $a, b \in Z_q^*$ and $P, Q \in G_1$, $e(aP, bQ) = e(P, Q)^{ab}$.
2. Nondegenerate: There exists a point P such that $e(P, P) \neq 1$.
3. Computable: There is an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_1$.



2 Complexity Assumptions

Definition 1 (q-strong Diffie-Hellman (q-SDH) Assumption [12]). *Given* $(P_1, P_2, \gamma P_2, \gamma^2 P_2, \ldots, \gamma^q P_2)$, *it is infeasible to compute* $\frac{1}{\gamma+x} P_1$, *where* $x \in Z_q^*$.

Definition 2 (Decision linear (DL) Assumption [8]) *Given* $P_1, P_2, P_3, aP_1, bP_2, cP_3$, *it is infeasible to decide whether* $a + b = c \bmod q$.

Definition 3 (Weak Bilinear Diffie-Hellman Exponent (WBDHE) Assumption [13]). *For unknown* $a \in Z_q^*$, *given* $Y, aY, a^2Y, .., a^lY, P \in G_1$, *it is infeasible to compute* $e(Y, P)^{\frac{1}{a}}$.

Definition 4 ((t,n)-general Diffie-Hellman Exponent (GDHE) Assumption [14]). *Let* $f(X) = \Pi_{i=1}^{r}(X + x_i)$ *and* $g(X) = \Pi_{i=1}^{n-r}(X + x_i')$ *be the two random univariate polynomials. For unknown* $k, \gamma \in Z_q^*$, *given*

$$G_0, \gamma G_0, ..., \gamma^{t-1} G_0, \gamma f(\gamma) G_0, P_0, ..., \gamma^{t-1} P_0, kg(\gamma) H_0 \in G_1 \text{ and}$$

$$e(G_0, H_0)^{f^2(\gamma) g(\gamma)} \in G_2,$$

it is infeasible to compute $e(G_0, H_0)^{kf(\gamma)g(\gamma)} \in G_2$.

IV. Design Model

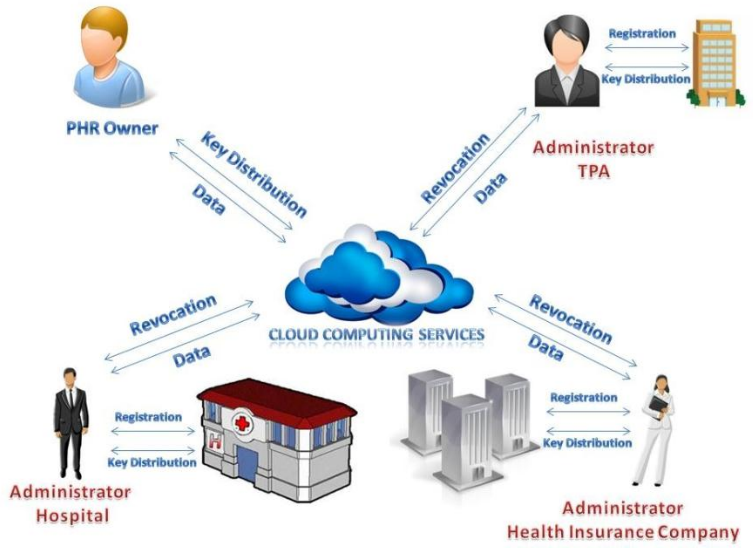
In this design model, a patient is considered to share his/her PHR in cloud computing architecture along with an example that Hospital uses a cloud to enable its physicians, surgeons and nurses in the same group to update/modify PHRs. Also Insurance company and TPA also access the Cloud to access PHRs. The design model consists of following entities as illustrated in Figure 1:

a. PHR owner
b. The cloud (Cloud Computing Services)
c. Group manager for the hospital (Hospital Administrator)
d. Group manager for Insurance company (Insurance company Administrator)
e. Group manager for TPAs (Third Party Administrator's administrator)

Here we assume that Cloud servers are honest but may be interested to know about PHRs. Meaning, cloud administrator may not add/delete/modify PHRs but view and interested to know the content of PHRs.

We assume Group manager is responsible for setting the parameters of user registration, user revocation, adopting policies and procedures which are set by the PHR owner and as part of policies and procedures , appropriate segregation of duties, user name standards, password policy, immediate revocation of access rights if a member quits. Hence the Group manager plays the role of administrator and he/she acts as an administrator for the particular organization and administrator is trusted by all the stake holders.

Fig 1: Proposed Design Model



We assume all the members are registered users by the group manager . All users signed Non Disclosure agreement, so that if any one leaks any information legal action would be proceeded. Also it is assumed that the users are provided with access rights on need to know basis, meaning Physicians may require access to update medical records where as Insurance company staff needs to know about the charges and TPA staff may be allowed to edit the amount for particular treatment. Since there are various groups, naturally the groups would be dynamic.

In the above proposed model, PHR owner encrypts the PHRs and distributes to all the administrators and places PHR in cloud. Each stake holder in respective group can be added/modified/deleted only by Group administrator. Through this model, even one of the stake holder resigns, PHR owner need not work on key management . Instead, Group administrators removes the user ID and revokes the user access rights. In case if the Group administrator resigns, then PHR owner needs to work on key management to create new set of keys and the new keys will be distributed.

V. Achievements of proposed design

The below listed are main achievements of the proposed design that include data confidentiality, access control , anonymity, traceability and efficiency

a. Data Confidentiality :

Data confidentiality means any unauthorized member including the cloud administrator should not view the content of PHR stored in the cloud. Appropriate access rights should be applied to the PHR's attributes. The challenge here is any new user should decrypt the data as soon as they got registered for the reason of availability and to maintain the confidentiality any user who quit could not view once they are removed from the group.

b. Access Control:

Access control has to achieve the purpose that the members should be accessing the PHRs only for relevant update /modification of PHR by respective stakeholders. Hence need to know access should be provided to all the stakeholders. Any unauthorized user at any point of time should not be accessing PHR for privacy reasons. Any stake holder who is not part of the attached organization should not be accessing PHR in private.

c. Anonymity:

Anonymity ensures that stakeholder can update the PHR in the cloud without revealing the real identity due to set of standard procedures adopted during creation of user ID. Only the group manager would know the real identity.

d. Traceability:

By enabling the effective audit schemes, the activities of all stakeholders will be tracked and hence the traceability would be achieved.

e. Efficiency:

As sited in [9], the method of using attribute based encryption of PHR involves dynamic key distribution and revocation which involves time consuming, cost involved and complexity. The proposed model is cost effective since the keys need not be changed and redistributed as when the stake holder quit his/her respective organization. Automatically the new user gains an access to the PHR before the owner shares the key since the administrator adds along with user ID. A high risk foreseen here is the situation when group administrator compromises the control. This could be mitigated through dual authentication methods and audit mechanisms which is assumed already present in the model.

VI. Conclusion

In this paper, we design a secure PHR accessing scheme, for dynamic stakeholders in an un trusted cloud. In this model, a stakeholder is able to update the PHR only to his/her appropriate section, thus maintaining privacy and without revealing identity to the cloud. This design supports Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant.

References:

[1]. Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, “Mona: Secure Multi-Owner Data Sharing for dynamic groups in the cloud “, published in IEEE Transactions on parallel and distributed systems, Vol 24, No.6, in June 2013

[2]. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,” Proc. IEEE INFOCOM ’10, 2010.

[3]. Encryption for Fine-Grained Access Control of Encrypted Data,” Proc. 13th ACM Conf. Computer and Comm. Security (CCS ’06), pp. 89-98, 2006.

[4]. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “Plutus: Scalable Secure File Sharing on Untrusted Storage,” proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5]. Securing Remote Untrusted Storage,” Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6]. D Boneh and M. Franklin, “Identity-Based Encryption from the Weil Pairing,” Proc. Int’l Cryptology Conf. Advances in cryptology (CRYPTO), pp. 213-229, 2001

[7]. D. Boneh, X. Boyen, and H. Shacham, “Short Group Signature,” Proc. Int’l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[8]. D. Boneh, X. Boyen, and E. Goh, “Hierarchical Identity Based Encryption with Constant Size Ciphertext,” Proc. Ann. Int’l Conf.Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[9]. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou, “ Scalable and Secure Sharing or Personal Health Records in Cloud Computing Using Attribute-Based Encryption”, published in Vol 24, No 1 of IEEE Transactions on Parallel and Distributed Systems in January 2013