International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Scalable and Secure Sharing of Personal Health records in Cloud Computing Using Attribute Based Encryption

Y. B. Gurav[1], Manjiri Deshmukh[2]

[1]Assistant Professor, Department of Computer Engineering, Pune University/PVPIT/JSPM, Bavdhan, Pune, Maharashtra, India

[2]Student, Department of Computer Engineering, Pune University/PVPIT/JSPM, Bavdhan, Pune, Maharashtra, India

Abstract: ***Personal health record is maintain in the centralize server to maintain patient's personal and diagnosis information. Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. The security schemes are used to protect personal data from public access. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing .In this paper we propose novel patient-centric framework and suite of mechanism for data access control to PHR's stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Data owner update the personal data into third party cloud data centers. Multiple data owners can access the same data values. Our scheme supports efficient on-demand user/attribute revocation.***

Keywords: Attribute-based encryption, cloud computing, data privacy, fine-grained access control, Personal health records, revocation

1. Introduction

Cloud computing is an emerging computing technology where applications and all the services are provided via Internet. It is a model for enabling on- demand network access to pool resources. Cloud computing can be considered as a computing paradigm with greater flexibility and availability at lower cost.

In recent year, Personal Health Record (PHR) has developed as the emerging trend in the health care technology and by which the patients are efficiently able to create, manage and share their personal health information. This PHR is now a day's stored in the clouds for the cost reduction purpose and for the easy sharing and access mechanism. The main concern about this PHR is that whether the patient is able to control their data or not. It is very essential to have the fine grained access control over the data with the semi-trusted server. But in this the PHR system, the security, privacy and health data confidentiality are making challenges to the users when the PHR stored in the third party storage area like cloud services. The PHR data should be secured from the external attackers and also it should be protect from the internal attackers such that from the cloud server organization itself. When the PHR owner upload the PHR data to the cloud server, the owner is losing the physical control over the data and thus the cloud server will obtain the access on the plain text data and it will make lots of security challenges to the PHR privacy and confidentiality. The encryption of data before outsourcing it to the third party is consider as the promising approach towards data security and confidentiality towards the third party storage. Privacy threats experienced by users of services offered by Apple Inc. Google Inc., Amazon Inc.[1] are clear indications that cloud is intrinsically insecure from a user's view point. Because users don't have access to cloud service providers internal operations preserving privacy of user in cloud environment is a challenge for researchers. Cloud computing services benefit from economies of scale achieved through versatile use of resources, specialization, and other efficiencies. The Internet has grown into a world of its own, and its huge space now offers capabilities that could support Physicians in their duties in numerous ways. In recent years, is an emerging trend and PHR is a patient-centric model of health information exchange and management. Generally, PHR service allows a user to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient.

2. Literature Survey

In cloud computing, there are different existing schemes that provide security, data confidentiality and access control. Users need to share sensitive objects with others based on the recipient's ability to satisfy a policy in distributed systems. This paper is mostly 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 [8] either incur high key manage-men overhead, or require encrypting multiple copies of a file using different users' keys. To improve upon the scalability of the above solutions, one-to-many en-crypt ion methods such as ABE can be used. In Goya let. all's seminal paper on ABE [11], data is encrypted under a set of attributes so that multiple users who possess proper keys can decrypt. This potentially makes encryption and key management more efficient [12]. Fundamental property of ABE is preventing against user collusion. At the early stages of the cloud computing and personal health record the traditional encryption techniques were applied to the personal health record and now days the advanced encryption techniques

such that attribute based encryption and its different variations are used.

ABE for Fine-grained Data Access Control:
Attribute-Based Encryption (ABE), a generalization of identity-based encryption that incorporates attributes as inputs to its cryptographic primitives. Data is encrypted using a set of attributes so that multiple users who possess proper can decrypt. Attribute-Based Encryption (ABE) not only offers fine-grained access control but also prevents against collusion.

Key Policy Attribute Based Encryption:
It is the modified form of the classical model of ABE. Exploring KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. Key Policy Attribute Based Encryption (KP-ABE) scheme is a public key encryption technique that is designed for one-to-many communications. This scheme enables a data owner to reduce most of the computational overhead to cloud servers. The use of this encryption scheme KP-ABE provides fine-grained access control.

Expressive Key Policy Attribute Based Encryption:
Expressive Key-Policy ABE, the encryption methods in clouds Attribute-based encryption (ABE), allows fine-grained access control on encrypted data. In the key policy Attribute based encryption, the primitive enables senders to encrypt messages with a set of attributes and private keys are associated with access tree structure that specifies which all the cipher-texts the key holder is allowed to decrypt. In most ABE systems, the cipher-text size grows linearly with the number of cipher-text attributes and the only known exceptions only support restricted forms of threshold access policies.

Cipher Text Policy Attribute Based Encryption:
Cipher-text Policy Attribute Based Encryption. In several distributed systems a user should only be able to access data if a user possesses a certain set of credentials or attributes.

Homo-marphic Encryption:
An encryption scheme has algorithm consists of three step.

1. Key Generation - creates two keys i.e. the privacy key prk and the public key puk.
2. Encryption - encrypts the plaintext P with the public key puk to yield cipher-text C.
3. Decryption - decrypts the cipher-text C with the privacy key prk to retrieve the plaintext P.
4. Evaluation - outputs a cipher-text C of f(P) such that Decrypt (prk,P) = f(P).

The scheme becomes homo-morphic if f can be any arbitrary function, and the resulting ciphertext of Eval is compact. That means it does not grow too large regardless of the complexity of function f. The Eval algorithm in essence means that the scheme can evaluate its own decryption algorithm.

Multi-authority Attribute Based Encryption
The multi-authority attribute based encryption scheme is an advanced attribute based encryption in which it will have many attribute authority for handling the different set of users from various domains [5]. In the PHR system the users will be from different domain like the doctors from health care organizations, the friends and family from personal relations and other users from insurance domain too. So each user will be having different access control mechanism based on the relation with the patient or owner. Thus the MA-ABE scheme will highly utilize.

3. Problem Statement

To implement scalable & secure sharing of personal health records in cloud computing using attribute based encryption.
To design efficient on-demand user revocation.

4. Implementation Details

A. Implementation steps

- Setup
- User Registration
- Key Generation
- Encryption
- Re-encryption
- Decryption

B. Why we need on Demand User Revocation

There are two conditions where we use the user revocation

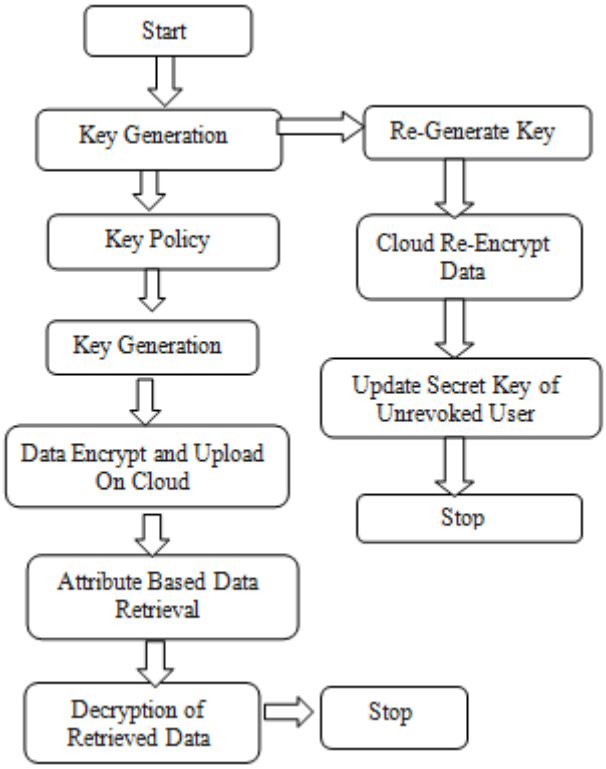
1. Whenever attribute changes or owner does not want to access parts of their PHR file anymore.
2. Whenever attribute changes.

C. Algorithm

Setup: Define attribute with P.K. and M.K. With ver=1

- Encrypt (Msg, policy,P.K.)→C.T.
- ReyKeyGen→Reykey rk,ver+1
- ReEnc(C.T., rk)→C.T.'
- KeyUpdate(S.K.,rk)→S.K.',ver+1

D. Design



Start

Cipher-text-Policy Attribute Based Encryption (CP-ABE)[6] is a cryptographic primitive for fine-grained access control of shared data. Each user is associated with a set of attributes and data are encrypted with access structures on attributes. A user is able to decrypt a cipher -text with the obtained attributes if it satisfy the cipher-text access structure. It explains patient access control policies such that everyone can download the encrypted data but only authorized users are allowed to decrypt it. In CP-ABE enables the authority to revoke user attributes with minimal effort and achieve this by uniquely integrating the technique of re-encryption with CP-ABE, and enable the authority to delegate most of laborious tasks to servers. It is provably securing against chosen cipher text attacks. It integrates the re-encryption technique with CP-ABE, and enables the authority to delegate most laborious tasks of user revocation to servers without leaking any confidential information to them. On each revocation event, the authority just generates several re- encryption keys and transmits them to servers. Servers will update secret keys for all users but the one to be revoked. CP-ABE is able to freely revoke any attribute of users at any time.

5. Conclusion

The personal health records are now considered as the emerging trend in the personal health information exchange field. And cloud computing storage and sharing service is highly utilized by the users. Cloud computing is increasingly used by healthcare service providers. Privacy is major issue while outsourcing healthcare data on cloud. The data security is the main privacy issue and the attribute based encryptions and its variations are applied for this security purpose. This paper supports efficient on-demand revocation using the CP-ABE technique.

6. Future Scope

In future, to provide high security and privacy for Personal Health Record (PHR), the existing Multi authority attribute based encryption could be further enhanced to proactive Multi authority attribute based encryption.

7. Acknowledgment

My sincere thanks to Prof. Y.B. Gurav sir for his helpful opinion and suggestion for the paper.

References

[1] Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in ACM CCS, ser. CCS ’08, 2008, pp. 417–426.
[2] Dong, G. Russello, and N. Dulay, “Shared and searchable encrypted data for untrusted servers,” in Journal of Computer Security, 2010.
[3] M. Li, S. Yu, N. Cao, and W. Lou, “Authorized private keyword search over encrypted personal health records in cloud computing,” in ICDCS ’11, Jun. 2011.
[4] “Google, microsoft say hipaa stimulus rule doesn’t apply to them,” http://www.ihealthbeat.org/Articles/2009/4/8/.
[5] H. L ¨ohr, A.-R. Sadeghi, and M. Winandy, “Securing the e-health cloud,” in Proceedings of the 1st ACM International Health Informatics Symposium , ser. IHI ’10, 2010, pp. 220–229.
[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in IEEE S& P ’07, 2007, pp. 321–334
[7] X. Liang, R. Lu, X. Lin, and X. S. Shen, “Ciphertext policy attribute based encryption with efficient revocation,” Technical Report, University of Waterloo, 2010.
[8] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, “Ciphertext-policy attribute-based threshold decryption with flex- ible delegation and revocation of user attributes,” 2009.
[9] M. Li, S. Yu, K. Ren, and W. Lou, “Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings,” in SecureComm’10, Sept. 2010, pp. 89–106.
[10] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in IEEE INFOCOM’10, 2010.
[11] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in ASIACCS’10, 2010.