INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

SECURE SHARING OF PERSONAL HEALTH RECORDS IN CLOUD COMPUTING USING ATTRIBUTE-BASED ENCRYPTION

SHITAL P. WADATKAR

Student, Department of Computer Science and Engineering, P.R.M.I.T & R, Bandera, Amravati

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: Personal Health Record (PHR) service is an emerging model for health information exchange. It allows patients to create, update and manage personal and medical information. Also they can control and share their medical information with other users as well as health care providers. PHR data is hosted to the third party cloud service providers in order to enhance its interoperability. 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 propose novel patient-centric framework and 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.

Keywords: Cloud computing, Data privacy, Fine grained access control, Attribute based encryption, Personal health records.

PAPER-QR CODE

Corresponding Author: MS. SHITAL P. WADATKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Shital P. Wadatkar, IJPRET, 2016; Volume 4 (9): 452-459

INTRODUCTION

Cloud computing means storing and accessing data and programs over the internet instead of using computer's hardware and software. Data security is the major problem in cloud computing. For security, different attribute based encryption schemes are used for encryption before outsourcing data to cloud server. 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. PHR data is hosted to the third party cloud service providers in order to enhance its interoperability. However, there have been serious security and privacy issues in outsourcing these data to cloud server. For security, encrypt the PHRs before outsourcing. So many issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for client's data, a novel patient centric framework is used.

2. OVERVIEW

The definition of PHR is heterogeneous and evolving. A personal health record (PHR) is simply a collection of information about a persons health. It is a tool for the excellent management of the health. J. Benaloh, [12], Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records has proposed a scheme in which a file can be uploaded without key distribution and it is highly efficient. But it is a single data owner scenario and thus it is not easy to add categories. C.Dong, [13] Shared and Searchable Encrypted Data for untrusted Servers, has explored that the data encryption scheme does not require a trusted data server. There is concern about security issues when outsource these data to the cloud server. Surveys shows that seventy five percentage people are not choose PHR system because they are concern about the security issues. For secure storing better method for designing PHR system is based on encryption method. Before outsourcing data to the third party different encryption methods are used. Public key Encryption (PKE) based scheme is one of the encryption method used for protecting data from third parties. But it has high key management overhead, or requires encrypting multiple copies of a file using different user's keys. Attribute based encryption is based on some access policies. These access policies are expressed based on the attribute of users or data which help to share PHR among set of users by encrypting the file under a set of attributes. Only authorized users with satisfying this access policy can access the PHR data. The main property of ABE is preventing against user collusion and the owner is not required to know the ACL.

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 finegrained 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.

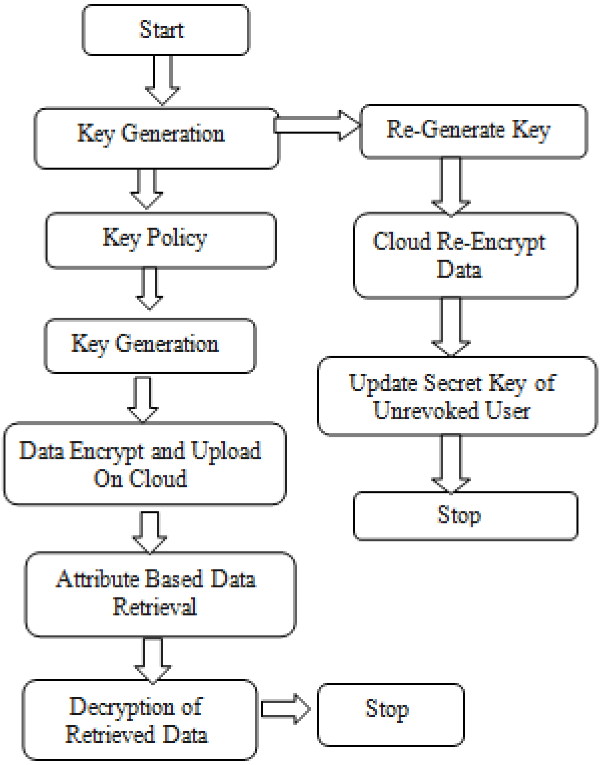
- ReyKeyGenReykey rk,ver+1

- ReEnc(C.T., rk)C.T.’

- KeyUpdate(S.K.,rk)S.K.’,ver+1

Paper

Design


Start
Key Generation
Re-Generate Key
Key Policy
Cloud Re-Encrypt Data
Key Generation
Update Secret Key of Unrevoked User
Data Encrypt and Upload On Cloud
Stop
Attribute Based Data Retrieval
Decryption of Retrieved Data
Stop

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.

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, “Ciphertextpolicy 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

12. J. Benaloh, M. Chase, E. Horvitz and K. Lauter, Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records, CCSW 09, 2009, pp. 103114

13. C. Dong, G. Russello and N. Dulay, Shared and Searchable Encrypted Data for Untrusted Servers, Journal of Computer Security, 2010.