ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Scalable And Secure Sharing Of Personal Health Records In Cloud Computing Using Multi Authority Attribute-Based Encryption

Satheesh.K[1], Ram kumar.A[2]

M.E. Arunai Engineering College Computer Science and Engineering, Thiruvannamalai, India[1]

Assistant Professor, Arunai Engineering College Computer Science and Engineering, Thiruvannamalai, India[2]

ABSTRACT: Personal Health Record (PHR) is maintained in the centralized server to maintain the patient's personal and PHR services are outsourced to third-party service providers. The main concern is about diagnosis information. The patient records should be whether the patients could actually control the sharing maintained with high privacy and security. The security schemes are used to protect the personal data from public access. Patient data can be accessed by many different people. Each authority is assigned with access permission for a particular set of attributes. The access control and privacy management is a complex task in the patient health record management process. Cloud computing is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers that are connected through a real-time communication network. It is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. Data owners update the personal data into third party cloud data centers. The novel patient-centric framework and a suite of data access mechanisms to control PHRs 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. Multiple data owners can access the same data values. The proposed scheme could be extended to Multi Authority Attribute Based Encryption (MA-ABE) for multiple authority based access control mechanism.

I. INTRODUCTION

Personal Health Record (PHR) is emerged as a patient- centric model of health information exchange. It enables the patient to create and control their medical data which may be placed in a single place such as data center. Due to the high cost of building of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the one hand, although there exist health care regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive Personal Health Information (PHI), the third -party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI In security based ensure privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. Hence we move to a new encryption pattern namely Attribute Based Encryption (ABE). In ABE, it is the attributes of the users or the data that selects the access policies, which enables a patient to selectively share their PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. As a result, the number of attributes involved determines the complexities in encryption, key generation and decryption. The Multi Authority Attribute Based Encryption (MAABE) scheme is used to provide multiple authority based access control mechanism. The PHR owner them self should decide how to encrypt their files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

access privileges when they feel it is necessary. The goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either need to access the PHR for personal use or professional purposes. Delineation and implementation of accepted standards for health-care data, accurate patient identification and record matching, and the definition of incentives for accelerated deployment of health information technology. In response to these challenges, we present in this paper an alternative option, the Health Record Banking (HRB) system. Emulating commercial banking, this approach uses health-record banks to serve the need for immediately accessible and secure data for diverse stakeholders.

II. RELATED WORK

In[1] Ming Li clients usually outsource their independence for these banks and a mechanism for fostering medical research. We conclude with 10 critical issues associated with the development and implementation of an HRB system, which require public data to the cloud storage servers to reduce the management costs. While those data may contain sensitive personal information, the cloud servers cannot be fully trusted in protecting them. Encryption is a promising way to protect the confidentiality of the outsourced data, but it also introduces much difficulty to performing effective searches over encrypted information. Most existing works do not support efficient searches with complex query conditions, and care needs to be taken when using them because of the potential privacy leakages about the data owners to the data users or the cloud server. Personal Health Record (PHR) as a case study,
we first show the necessity of search capability authorization that reduces the privacy exposure resulting from the search results, and establish a scalable framework for Authorized Private Keyword Search (APKS) over encrypted cloud data. We then propose two novel solutions for APKS based on a recent discussion. This paper describes the technology namely Health Record Banking (HRB). In [3] Liu, Z proposed the scheme called Clinical Document Architecture (CDA). Here X-PAT, a platform-independent software prototype that is able to manage patient referral multimedia data in an intranet network scenario according to the specific control procedures of a healthcare institution. It is a self- developed storage framework based on a file system, implemented in extensible Markup Language (XML) and PHP Hypertext Preprocessor Language, and addressed to the requirements of limited-dimension healthcare entities (small hospitals, private medical centers, outpatient clinics, and laboratories). In X-PAT, healthcare data descriptions, stored in a novel Referral Base Management System (RBMS) according to Health Level 7 Clinical Document Architecture Release 2 cryptographic primitive, Hierarchical Predicate (CDA R2) standard, can be easily applied to the Encryption (HPE). Our solutions enable efficient multi- dimensional keyword searches with range query, allow delegation and revocation of search capabilities. Moreover, we enhance the query privacy which hides users' query keywords against the server. We implement our scheme on a modern workstation, and experimental results demonstrate its suitability for practical usage. In this paper the technology used is Hierarchical Predicate Encryption (HPE). In [2] van den describes that the No unified, functioning system currently exists for the exchange of comprehensive health-care information across the wide spectrum of health-care networks. Regional health information organizations (RHIOs) and a national health information network (NHIN) have been proposed as vital building blocks in providing such a system, but these face many challenges, including specific data and organizational procedures of a particular healthcare working environment thanks also to the use of standard clinical terminology. Managed data, centralized on a server, are structured in the RBMS schema using a flexible patient record and CDA healthcare referral document structures based on XML technology. A novel search engine allows defining and performing queries on stored data, whose rapid execution is ensured by expandable RBMS indexing structures. Healthcare personnel can interface the X-PAT system, according to applied state-of-the-art privacy and security measures, through friendly and intuitive Web pages that facilitate user acceptance.

III. BACKGROUND

In this section, we are going to present our cloud storage model and the assumptions we had made for this paper.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Assumptions

1. The cloud is a honest one in the sense that cloud service providers can be only able to read the contents and cannot be able to modify it. This is a valid assumption that can be made in order to hold the algorithm good.
2. Users can be able to read or write or can perform both the read and write operations on the data present in the cloud.
3. The Secure Shell Protocol SSH is used to communicate between the users and the cloud. All the communication is via this particular protocol.

Access Control Policy

Multi-Authority Attribute based access policy is used in which the data are provided with access policy to data owners and users are given with attributes based on which the files are accessed.

Encryption technique

Attribute based encryption is used to encrypt the files. In this attribute based encryption, the data which are to be given security is encrypted under some access policy and then stored in the cloud. Then the users are given with a set of attributes and their corresponding keys. The individual data owners who are authorized rights to decrypt the files if and only if the corresponding set of specified multi-attributes matches with the access policy.

IV. DESIGN GOALS

Our main goal of this paper is to provide the security to the data files present in the cloud server. Especially we allow the data owner to provide an access policy for each data. The users are given with a set of attributes and their corresponding keys. The individual users can only decrypt the files if and only if the corresponding set of attributes matches with the access policy. In addition to that, we handle the users who are revoked. That is users who are not authorized but once upon a time authorized must not be able to access the data.

Maintaining Confidentiality

This property assures that the unauthorized users are not allowed to read or modify the data file and thus maintain the confidentiality of the data file in the cloud.

Data Access

The data access can be described in two ways. First, any member of the group can access the data present in the cloud. Second, unauthorized and revoked users cannot gain access to the files of the cloud resources.

V. OUR PROPOSED SCHEME

Main Idea

The Personal Health Records are maintained in a data server under the cloud environment. A novel framework of secure sharing of personal health records has been proposed in this paper. Public and Personal access models are designed with security and privacy enabled mechanism. The framework addresses the unique challenges brought by multiple PHR

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

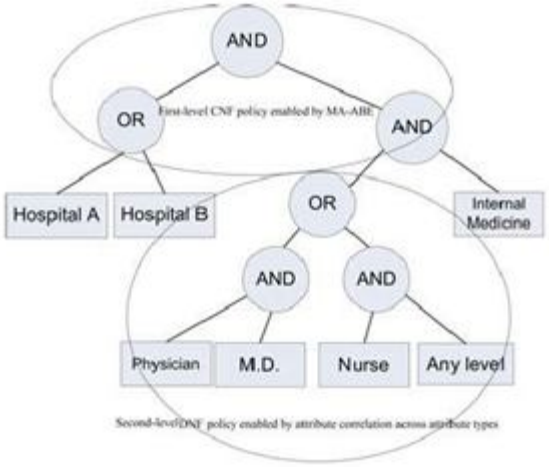
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

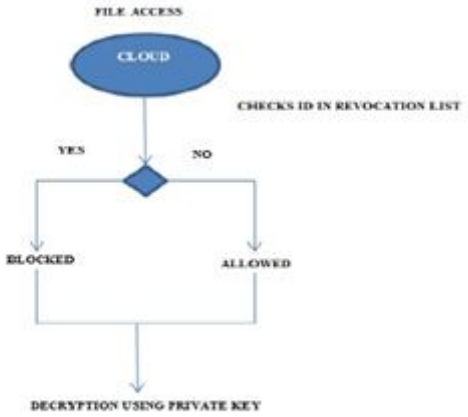
Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

owners and users, in that the complexity of key management is greatly reduced. The attribute-based encryption model is enhanced to support operations with MAABE. The System is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy. In future, to provide high security and privacy for Personal Health Record (PHR)





Scheme Description

This section describes the step by step process of implementation of each and every module of the algorithm.

System Initialization

The administrator is responsible for the system initialization.
1. Administrator creates a master key
2. This Master key is used to access the files

File Creation

User revocation.

Here, we consider revocation of a data reader or her attributes/access privileges. There are several possible cases:

1. Revocation of one or more role attributes of a public domain user;
2 . Revocation of a public domain user which is equivalentto revoking all of that user's attributes. the server to improve efficiency.
3. Revocation of a personal domain user's access Privileges
1.The file is created by the administrator.
2. Once the file is created, a file id is created.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

4. Revocation of a personal domain user. These can be initiated through the PHR owner's client application in a similar way.

User Registration

1. The new users are registered in the cloud.
2. Once the user gets the registration message to the cloud, the cloud sends a private key to the user
3. This private key is associated with a set of attributes.
4. The individual users can only decrypt the files if and only if the corresponding set of attributes matches with the access policy. .

Write access control.

Prevent the unauthorized contributors to gain write-access to owners PHRs, while the legitimate contributors should access the server with accountability.

File Storing

1. The file which is created is encrypted using attribute based encryption.
2. The cipher-text is stored in the cloud
3. Along with the cipher-text, the file id, the group id, and a group signature is stored.

File Read Access

1. To read the data file in the cloud, the private key of the user is used.
2. This private key is initiated and created by the cloud during user registration.
3. Using this private key, the user can decrypt the files stored in the cloud.
4. Before that, the cloud checks for the revocation list.
5. The user id must not be present in the revocation list.
6. If the user id is present in the list, then the user is not allowed to read the data file in the cloud. The user is considered as an unauthorized user.
7. Else the user is allowed to access and read the cloud.

The users can only decrypt the files if and only if the corresponding set of attributes matches with the access policy.

VI. PERFORMANCE ANALYSIS

As the cloud performs various operations, it is On-demand revocation.
Whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute. This is usually called attribute revocation, and the corresponding security property is forward secrecy [23]. There is also user revocation, where all of a user's access privileges are revoked.

File Write Access

1. To write or modify a file in the cloud, the user also uses the private key. 2. Before that, the cloud checks for the revocation list.
3. The user id must not be present in the revocation list.
4. If the user id is present in the list, then the user is not allowed to modify the data file in the cloud. The user is considered as an unauthorized user.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

5. Else the user is allowed to access and modify the cloud.
6. Once the data is modified, the data file must be uploaded into the cloud.
7. Now the cloud will check and verify for the signature.
8. If the signature is verified, the data file is uploaded successfully into the cloud.
9. This scheme of using revocation list reduces the overhead of updating the keys of every user when there is a revocation or a new participation much speeder in its performance. Cloud has a distributed environment. As the computations are shared between the user and the administrator and the cloud, the performance of the algorithm is good.

VII. COMPUTATION COMPLEXITY

Lazy-revocation method greatly reduces the cost of revocation, because it aggregates multiple ciphertext/key update operations, which amortizes the computations over time the various functionalities and the computations are shared between the users of the cloud namely the cloud, the administrator, and the user, the computation overhead is minimized. During revocation, it is not necessary to update the keys of every user when there is a staff revocation happens. Instead we have a revocation list which consists of the users who are revoked. Based on this, the access is determined

VIII. CONCLUSION AND FUTURE WORK

In this paper System is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy. 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 Data Confidentiality and Integrity is a major concern. We mainly concentrate on business cloud where various organizations store their data about their project in the cloud. We have analyzed the security of our algorithm and also the efficiency.

REFERENCES

[1] Ming Li "Authorized private keyword search over encrypted personal health records in cloud computing"

[2] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private KeywordSearch over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems(ICDCS '11), June 2011.

[4] "The Health Insurance Portability and Accountability Act,"http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp,2012.

[5] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply toThem," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.[6] "At Risk of Exposure - in the Push for Electronic Medical Records,Concern Is Growing About How Well Privacy Can Be Safeguarded," http://articles.latimes.com/2006/jun/26/health/
he-privacy26, 2006.

[7] K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287, Feb. 2001.

[8] 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.

[9] 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[10] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.

[11] 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.

[12] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm. Magazine, vol. 17,no. 1, pp. 51-58, Feb. 2010.

[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008. [14] 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.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp.[1] Information, Computer and Comm. Security (ASIACCS '10), 2010.