IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

SCALABLE AND SECURE SHARING OF PERSONAL HEALTH RECORDS INCLOUD COMPUTING USING ATTRIBUTE-BASED ENCRYPTION

M.RAJATHI[1] and Mrs.S.SUGA D H I[2] [1]Final Year PG Student, [2]Assistant Professor.
Department of Computer Science,
G. Venkataswamy Naidu College,Kovilpatti,
TamilNadu, India.

ABSTRACT_ 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. To assure the patients' control over access to theirown PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, 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. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to 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. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

KEYWORDS_ PERSONAL HEALTH RECORDS,CLOUD COMPUTING,DATA PRIVACY,FINE-GRAINED ACCESS CONTROL,ATTRIBUTE-BASED ENCRYPTION.

INTRIDUCTION_ In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient 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. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, manyPHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing PHRs in cloud computing have been proposed in.

While it is exciting to have convenient PHR services for everyone, there are many security and privacy risk which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing 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 healthcare 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 ofthe PHI. As a famous incident, a Department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans, includingtheir social security numbers and health problems was stolen by an employee who took the data home without authorization. To ensure patient- centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi- trusted servers.

EXSITING SYSTEM

While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks. Which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information(PHI), especially when they are stored on a third-party server which people may not fuly trust.

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.

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

Modules Description

Registration

In this module normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files– leaf nodes is atomic file categories while internal nodes are compound categories.

Dark boxes are the categories that a PSD's data reader has access to. Two ABE systems are involved: for each PSD the revocable KP-ABE scheme is adopted for each PUD, our proposed revocable MA-ABE scheme.

PUD-public domains
PSD-personal domains
-attribute authority
-ABE - multi-authority ABE
-ABE - key policy ABE

Upload files

In this module, users upload their files with secure key probabilities. The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file encrypted both under a certain fine grained model.

ABE for Fine-grained Data Access Control

In this module ABE to realize fine-grained access control for outsourced data especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs).

Setup and Key Distribution

In this module the system first defines a common universe of data attributes shared bye very PSD, such as "basic profile", "medical history", "allergies", and "prescriptions". An emergency attribute is also defined for break-glass access. Each PHR owner's client application generates its corresponding public/master keys. The public keys can be published via user's profile in an online healthcare social-

network (HSN).

There are two ways for distributing secret keys.

PHR service, a PHR owner can specify the access privilege of a data reader in her PSD, and let her application generate and distribute corresponding key to the latter, in a way resembling invitations in Google Doc.

THE .NET FRAMEWORK

The .NET Framework is a new computing platform that simplifies application development in the highly distributed environment of the Internet.

OBJECTIVES OF. NET FRAMEWORK

- To provide a consistent object-oriented programming environment whether object codes is stored and executed locally on Internet-distributed, or executedremotely.
- To provide a code-execution environment to minimizes software deployment and guarantees safe execution of code.
- Eliminates the performance problems

There are different types of application, such as Windows-based applications and Web-based applications.

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.

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. 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. Further- more, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we show that our solution is both scalable and efficient.

References

[1] Boldyreva, V. Loyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS '08, 2008, pp. 417–426.

[2] Dong, G. Russell, and N. Duly, "Shared and searchable encrypted data for unfrosted 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 hippie stimulus rule doesn't apply to them," http://www.ihealthbeat.org/Articles/2009/4/8/.

[5] H. L ¨ohm, A.-R. Sadeghi, and M. Wind, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium , ser. IHI '10, 2010, pp. 220–229.

[6] J. Bettencourt, A. Shay, and B. Waters, "Cipher textpolicy attribute-based encryption," in IEEE S& P '07, 2007, pp. 321–334

[7] X. Liang, R. Lu, X. Lin, and X. S. Sheen, "Cipher text policy attribute based encryption with efficient revocation," Technical Report, University of Waterloo, 2010.

[8] L. Ibrahim, M. Petkovic, S. Nikola, P. Harte, and W. Joker, "Cipher text-policy attribute-based threshold decryption with flex- able delegation and revocation of user attributes," 2009.

[9] M. Li, S. Yu, K. Ran, 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.