International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP 711-715

ENFORCING DATA SECURITY FOR SECURED SHARING OF DATA IN CLOUD

Monika Kute[1], Vaibhavi Lad[2], Seemantini Naikade[3,] Yogesh Sayaji[4]
(Dept. of IT, Dr.D.Y.Patil College of Engg Pune, Savitribai Phule Pune University)

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 their own 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 project, 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.

I. INTRODUCTION

This paper is based on the Personal Health Record (PHR). 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 authorized users control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. A PHR service allows a patient and doctor 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. This data is accessible to only authenticated users. In case any third party (unauthorized user) tries access this data then a security message will be generated and sent to the authorized user whose data has been accessed by the unauthorized user. Due to this stored data, doctors can access information about the patient and vice versa. Also the insurance company can access the data of the patient according to their requirement. And even the receptionist can check the schedule, appointments, billing, manage records etc accordingly. This project is developed in Java which provides best features for web development. It is one of the best languages in web development trend. Even if there are many web development technologies and languages were available, this language provides best features for dynamic control and securities.

II. RELATED WORK

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], [10] either incur high key management 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 encryption methods such as ABE can be used in which reverse cycle encryption algorithm is used [13]. In Goyal et al.'s seminal paper on

ABE [11], data are 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]. A fundamental property of ABE is preventing against user collusion.

III. PROPOSED METHOD

Framework for patient centric, secure and scalable PHR sharing in this section, we describe our novel patient-centric secure data sharing framework for cloud-based PHR systems.

3.1 Problem Definition :

We consider a PHR system where there are multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage, and delete it. There is a central server belonging to the PHR service provider that stores all the owners PHRs. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data. A typical PHR system uses standard data formats. For example, continuity-of-care (CCR)(based on XML data structure), which is widely used in representative PHR systems including Endive , an open source PHR system adopted by Boston Children's Hospital. Due to the nature of XML, the PHR files are logically organized by their categories in a hierarchical way.

3.2. Overview of Our Framework:

The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains and personal domains) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses, and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government, or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner.

3.2.1. Security Model:

In this paper, we consider the server to be semi trusted, i.e., honest but curious. That means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collude with other users, or even with the server. In addition, we assume each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols.

3.2.2. Requirements:

To achieve PHR sharing, a core requirement is that each authorized users can control their own PHR documents. Especially, user-controlled read/write access and revocation are the two core security objectives for any electronic health record system, pointed out by Mandletal.in as early as 2001. The security and performance Requirements are summarized as follows:

- Data confidentiality :

Unauthorized users (including the server) who do not possess enough attributes satisfying the access policy or do not have proper key access privileges should be prevented from decrypting a PHR document, even under user collusion. Fine-grained access control should be enforced, meaning different users are authorized to read different sets of documents.

- 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. There is also user revocation, where all of a users access privileges are revoked.

- Write access control :

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

- Data access policy :

The data access policies should be flexible, i.e., dynamic changes to the predefined policies shall be allowed, especially the PHRs should be accessible under emergency scenarios.

- Scalability, efficiency, and usability :

The PHR system should support users from both the personal domain and public domains. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. Additionally, the owner's efforts in managing users and keys should be minimized to enjoy usability.

IV. SYSTEM WORKFLOW

The user has to first register then the user data will be generated. Then the user has to login filling the correct information according to the registration. Then all the information of the user is concatenated in one string. Characters are selected randomly from the generated string and the key is generated from these. After key generation process, attributes from messages are selected. These attributes are replaced with special characters and are saved in the cloud.

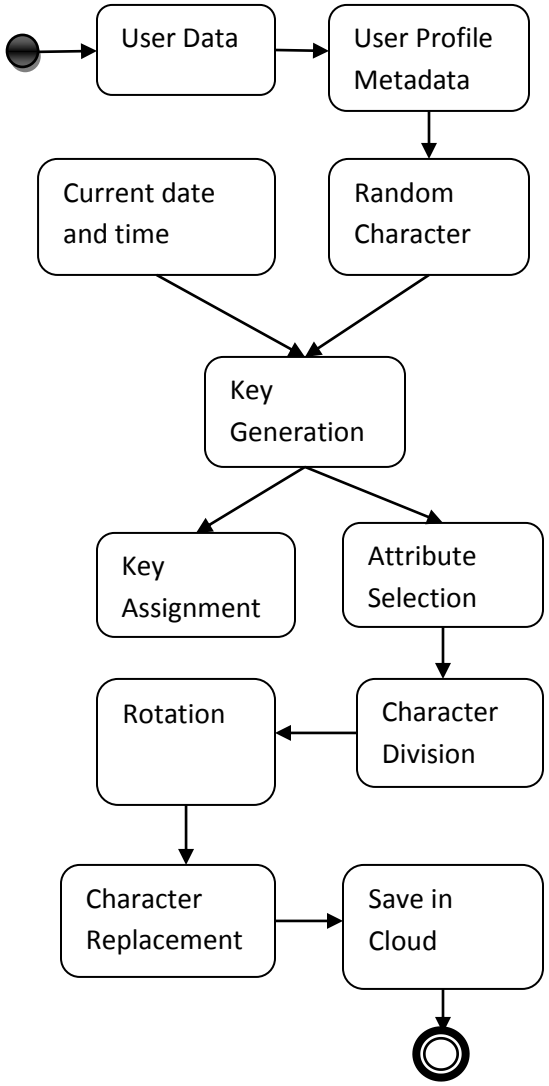

Fig.1: System Workflow

V. CONCLUSION

This project proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, users should have complete control of their own privacy through attribute-based encryption of PHR files to allow fine-grained access.

REFERENCES

[1]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," Proc. Sixth Int'lI CST Conf. Security and Privacy in Comm. Networks (Secure Comm '10),pp. 89-106, Sept. 2010.

[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 Keyword Search 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 to them," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6] "At Risk of Exposure-in the Push for Electronic record, concern is growing about how well Privacy can Be Safeguarded,"http://articles.latimes.com/2006/jun/26/health/he_pravacy26,2006

[7] K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical RecordsAccessible 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.

[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 WirelessBody Area Networks," IEEE Wireless Comm. Magazine, vol. 17,no. 1, pp. 51-58, Feb. 2010.

[13] Ebenezer R.H.P. Isaac, Joseph H.R. Isaac and J. Visumathi Jeppiaar Engineering College Chennai, Tamil Nadu, India "Reverse Circle Cipher for Personal and Network Security"