Enhancing Security of Attribute Based Encryption For Secure Sharing of Personal Health Records in Cloud Computing

Engineering

KEYWORDS : Personal health records; attribute based encryption; cloud computing

Jerusha Raichie George S4 M.Tech, Dept of Computer Science & Engineering, N.S.S College of Engineering, Palakkad, Kerala, India.

Miss Sruthy Manmadhan Assistant Professor, Dept of Computer Science & Engineering, N.S.S College of Engineering, Palakkad, Kerala, India.

ABSTRACT

Cloud computing, is an emerging computing environment which allows users to remotely store the data in one centralized place. This facilitates on demand scalable services as well as efficient management and sharing of data. 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 and unauthorized parties .To assure the patients' control over access to their own PHRs, a promising method is 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. A novel patient centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted server are needed. To achieve fine-grained and scalable data access control for PHRs, Attribute Based Encryption (ABE) technique is used to encrypt each patient's PHR file. In order to enhance the security an external USB is also used.

I. Introduction

One of the biggest advantages of cloud computing is that users can access data stored in the cloud anytime and anywhere using any device, such as thin clients with minimum bandwidth, processing, and memory capabilities. Considering these merits of cloud computing an idea of PHR model is put forth. Personal health record (PHR) is an upcoming patient-centric model for storing patient's e-record in one centralised place. It allows patients to create, manage, control and share their health information with other users as well as health care providers. The other long term benefits are easy management of personal health information, freedom of sharing only relevant information with authorized care providers and lastly to maximize health benefits. For better usage patient can upload health measurements directly from their devices or import their health records from hospital EHR System. Considering the value of sensitive PHI and as cloud services do not come under covered entities [1], there exist health care regulations such as HIPAA [2] which is recently amended to incorporate business associates rules. Current date leading third party service providers are Microsoft HealthVault1, Google Health or Web MD. 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. A best suited approach would be to encrypt the data before outsourcing. A PHR should only be available to set of users with the alternative decryption key while it should not be exposed to rest of the users. The patient shall retain the rights to grant as well as revoke the access rights [3].the users can be further categorized as Personal and Professional. Personal include family members and friends while Professional cover the large scope like medical doctors, pharmacists, and researchers, etc. Professional category requires potentially large scale key management if done by single authority. To avoid this problem a PHR system with multiple owners is put forth [4], [5]. They may encrypt according to their own ways, possibly using different sets of cryptographic keys. The paper focuses on patient centric and secures sharing of PHR records on a semi trusted server using attribute based encryption and an external USB to enhance security.

II. related works

In the past, health care providers have stored medical records of their patients on paper locally. This allowed a controlled environment with easy management of data privacy and security. The increasing use of personal computers and modern information technology in medical institution allowed for a moderate effort to manage privacy and confidentiality of individual medical records. This was due to the decentralised and locally managed infrastructure of each institution. Outsourcing leads to a complex system where privacy sensitive data are stored and processed at many different places. Hence it became attractive to store and process healthcare data in the cloud. Such e-health systems promise a more cost effective service and improved service quality but the complexity to manage data securely and privacy increases. In commercial systems like Google Health, Microsoft HealthVault and ICW LifeSensor, patients store their health-related data on certain web servers called Personal Health Record (PHR). The patients can track, collect, and manage the information about their health at online web sites.

In contrast to PHRs, which are managed by the patients, Electronic Health Record (EHR) is managed by health professionals. The problems of e-health clouds are data storage and processing management of e-health infrastructure, usability and user experience. A secure e-health infrastructure to ensure fundamental security and privacy properties was proposed [6]. Security in e-health systems should be enforced by encryption as well as access control. The patients must be able to generate and store encryption keys, so that the patients' privacy is protected. But encryption would interfere with the functionality of the system. A Patient Controlled Encryption (PCE) was proposed as a solution to secure and private storage of patients' medical records. PCE allows the patient to selectively share records [4].

Then data encryption scheme that does not require a trusted data server was proposed. The server can perform encrypted searches and updates on encrypted data without knowing the plaintext or the decryption keys [7]. A scalable framework for Authorized Private Keyword Search (APKS) over encrypted cloud data was proposed in [8]. With encrypted data, keyword search becomes a challenging issue. In Ciphertext-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the ciphertext is associated with an access structure or decryption policy over attributes. The user can decrypt the ciphertext if and only if the attribute set of his secret key satisfies the decryption policy specified in the ciphertext. In key- policy ABE, the encryptor exerts no control over who has access to the data she encrypts, except by her choice of descriptive attributes for the data[9],[10].

Another form of CP-ABE is multi-authority CP-ABE. It allows patients to encrypt the data according to an access policy over a set of attributes issued by two trusted authorities: the trusted authority (TA1) of the professional domain (PD) and the trusted authority (TA2) of the social domain (SD). The patient himself could also take the role of TA2. TA1 will authenticate users of the professional domain, and issue secret keys based on their attributes, while the patient might use the reputation of the users of the social domain to generate appropriate secret keys [11].

Another system was proposed to maintain electronic medical record (EMR) availability even when the providers are offline. For this, ABE was used which facilitates granular role-based and content- based access control for EMRs, without the need for a single, vulnerable centralized server [12]. In a multi-authority ABE system, there will many attribute authorities, and many users [13]. To overcome the drawbacks of [13], a new multi-authority scheme was proposed without a trusted authority and with an anonymous key issuing protocol which allows multi-authority ABE with enhanced user privacy [14].

Then CP-ABE scheme with efficient revocation was proposed. In this malicious users can be efficiently revoked [15]. An attribute-based access control scheme using CP-ABE with efficient attribute and user revocation capability for data outsourcing systems was proposed. The scheme had several advantages with regard to the security and scalability compared to the previous revocable CP-ABE schemes. It allows a data owner to define the access control policy and enforce it on his outsourced data [16].

III. attribute based encryption

In ABE a sender can encrypt a message specifying an attribute set and a number *d*, such that only a recipient with at least *d* of the given attributes can decrypt the message [6]. In order to protect the personal health data stored on a semi-trusted server, attribute-based encryption (ABE) is adopted as the main encryption primitive. ABE enables a patient to share the encrypted records among the selected users.

A. Key policy attribute based encryption(KP-ABE)

In KP-ABE cipher texts are designated with sets of attributes and private keys .Private keys are related with access structures that in turn specifies which type of cipher texts the key can decrypt.

B. Ciphertext policy attribute based encryption(CP-ABE)

In a CP-ABE scheme, every ciphertext is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a ciphertext only if the set of attributes associated with the user's private key satisfies the access policy associated with the ciphertext. CP-ABE works in the reverse way of KP-ABE.

IV. Proposed PHR framework

A. 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. The users may come from various aspects; for example, a friend, a caregiver or a researcher. 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.

B. Implementation details

(1) For actual encryption/decryption of data RSA algorithm is used.

(2) Dividing system into domains: Aim 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 (PUDs) and personal domains (PSDs) 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. Both types of security domains, utilize ABE to realize cryptographically enforced, patient-centric PHR access.

(3) Encryption of PHR and Access rules: The files which are encrypted using ABE are uploaded on server by the owner. Each owner PHR files are encrypted on the basis of certain fine grained and role based access policy. Encrypted files can be decrypted only by authorized users, excluding the server.

(4) Policy Updates: Sharing policy for an existing PHR is done by PHR owner by updating the attributes (or access policy) in the cipher text. The supported operations like add/delete/modify can be performed by server on behalf of the user

(5) Break-glass: A break glass concept is used in case of emergency. Break glass allows bypassing the regular access policies and accessing the PHR record through emergency department (ED) .For this scheme PHR access rights are delegated to emergency department beforehand. To prevent from abuse of break-glass option, the emergency staffs needs to contact the ED to verify identity and emergency situation, as well as obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED.

(6) Security enhancement: In order to enhance the security an external USB is also used. When a PHR user registers, he is requested to connect a USB. The serial number of the USB is read and stored in the database along with other details. The USB is necessary thereafter to sign in. When a user log in, he is asked to connect the USB and the serial number of the connected USB is checked with already saved serial number. If the two serial numbers matches, then user can log in, otherwise the user will be blocked.

V. CONCLUSION

In this paper, a novel framework for secure sharing of personal health records in cloud computing is proposed. Considering partially trustworthy cloud servers, to fully realize the patient-centric concept, patients' should have complete control of their own. To achieve this, PHR files are encrypted. Attribute Based Encryption (ABE) is used to encrypt the PHR data, 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. PHR data will be accessible by only those who possess the proper key. Also the security of Attribute Based Encryption is enhanced by using an external USB. One will not be able to access PHRs without the USB device.

REFERENCE

[1] “Google, Microsoft say hipaa stimulus rule doesn’t apply tothem,” http://www.ihealthbeat.org/Articles/2009/4/8/. | | [2] “The health insurance portability and accountability act.”[Online].Available:http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp | | [3] 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, p. 283, Feb. 2001 | | [4] 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. | | [5] 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. | | [6] H. Lohr, 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. | | | [7] C. Dong, G. Russello, and N. Dulay, “Shared and Searchable Encrypted Data for Untrusted Servers,” J. Computer Security, vol. 19, pp. 367-397, 2010. | | [8] 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. | | [9] 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. | | [10]. J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy (SP ’07), pp. 321-334, 2007. | | [11]. L. Ibraimi, M. Asim, and M. Petkovic, “Secure Management of Personal Health Records by Applying Attribute-Based Encryption,” technical report, Univ. of Twente, 2009. | | [12] J.A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson, and A.D. Rubin, “Self-Protecting Electronic Medical Records Using Attribute-Based Encryption,” Cryptology ePrint Archive, Report 2010/565, http://eprint.iacr.org/, 2010. | | [13] Melissa Chase. Multi-authority Attribute Based Encryption. In TCC, volume 4392 of LNCS, pages 515–534. Springer 2007. | | [14] M. Chase and S.S. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” Proc. 16th ACM Conf. Computer and Comm. Security (CCS ’09), pp. 121-130, 2009. | | [15] X. Liang, R. Lu, X. Lin, and X.S. Shen, “Ciphertext Policy Attribute Based Encryption with Efficient Revocation,” technical report, Univ. of Waterloo, 2010. | | [16] J. Hur and D.K. Noh, “Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,” IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011. |