ISSN:2320-0790

An International Journal of Advanced Computer Technology

Improved Security of Attribute Based Encryption for Securing Sharing of Personal Health Records

Able E Alias[1], **Neethu Roy**[2]

[1]Research Scholar, Department of Information Technology, ICET Mulavoor, Ernakulum, India

[2]Asst.Professor, Department of Information Technology, ICET Mulavoor, Ernakulam, India

Abstract: Cloud computing servers provides platform for users to remotely store data and share the data items to everyone. Personal health record (PHR) has emerged as a patient –centric model of health information exchange. Confidentiality of the shared data is the major problem when patients uses the commercial cloud servers because it can be view by everyone., to assure the patient's control over access to their own medical records; it is a promising method to encrypt the files before outsourcing and give access control to that data. 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 a high degree of patient privacy is guaranteed by exploiting multi-authority ABE. Divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users.

Keywords: Secure sharing, Multi-Authority Attribute Based Encryption, Key-Policy Attribute Based Encryption, Personal Health Record, Cloud Computing.

INTRODUCTION

Personal health record 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. The main objective is to secure personal health records using multi authority ABE. That is multiple authorities can access the PHR without affecting the security features. For handling emergency situations, emergency department is implemented with external security.

Normally introducing 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 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 PHI, the third party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI. As a famous incident, a Department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans, including their 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. For this reason a new system is proposed that ensures the security of PHR. That should be done using ABE Algorithm.

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 decentralized and locally manage infrastructure of each institution.

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 [1]. 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 [2].

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 [3]. A scalable framework for Authorized Private Keyword Search (APKS) over encrypted cloud data was proposed in [4]. With encrypted data, keyword search becomes a challenging issue. In Cipher text-Policy Attribute-Based Encryption (CP-ABE), a user secret key is associated with a set of attributes, and the cipher text is associated with an access structure or decryption policy over attributes. The user can decrypt the cipher text if and only if the attribute set of his secret key satisfies the decryption policy specified in the cipher text. 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[5],[6]. 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

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 [7]. In a multi-authority ABE system, there will many attribute authorities, and many users [8]. To overcome the drawbacks of [8], 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 [9].Then CP-ABE scheme with efficient revocation was proposed. In this malicious users can be efficiently revoked [10]. 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 [11].

ATTRIBUTE BASED ENCRYPTION

The concept of ABE was introduced along with another cryptography called fuzzy identity-based encryption (FIBE) [6] by Sahai and Waters. Both schemes are based on bilinear maps (pairing). In ABE system, users' private keys and cipher text are labeled with sets of descriptive attributes and access policies respectively, and a particular key can decrypt a particular cipher text only if associated attributes and policy are matched

Key-Policy Attribute-Based Encryption

The key-policy attribute-based encryption (KP-ABE) was first introduced in 2006 by Goyal et al. [5] In this cryptography system, cipher text are labeled with sets of attributes. Private keys, on the other hand, are associated with access structures A. A private key can only decrypt a cipher text whose attributes set is authorized set of the private key's access structure. KP-ABE is a cryptography system built upon bilinear map and Linear Secret Sharing Schemes.

Multi-Authority attribute-Based encryption

In a multi-authority ABE system[9], we have many attribute authorities, and many users. There are also a set of system wide public parameters available to everyone (either created by a distributed protocol between the authorities). A user can choose to go to an attribute authority, prove that it is entitled to some of the attributes handled by that authority, and request the corresponding decryption keys. The authority will run the attribute key generation algorithm, and return the result to the user. Any party can also choose to encrypt a message, in which case he uses the public parameters together with an attribute set of his choice to form the cipher text. Any user who has decryption keys corresponding to an appropriate attribute set can use them for decryption.

PROPOSED PHR FRAME WORK

The operations of proposed medical record sharing system combine KP-ABE and Multi-Authority ABE and traditional cryptography, allowing patients to share their medical records. These operations can be classified into following modules: In this section we discuss main module design concept for sharing of medical records using Attribute based encryption – (KP-ABE and Multi Authority-ABE).

Modules of the system are:

System Set-Up and Key-Generation

As system is divided into two domains, both domains has different procedure for Set-up and Key Generation. In Set-Up public and master parameters are generated using RSA algorithm which are , used for key generation, encryption and decryption.

*Personal Domain :*The system first defines a common universe of data attributes shared by every PSD, such as “personal info”, “medial history”, “allergies”, and rescriptions” “emergency”, “friend” “relative” , “emergency”. An emergency attribute is also defined for break-glass access. Each data owner’s client application generates its corresponding public/master keys using Key-Policy attribute Based Encryption. The public keys can be published with help of system provided by service provider. Data Owner specify the access policy of data reader in her personal domain, and generates secret key using Key-Policy attribute Based Encryption. Personal domain user obtains secret key from the data owner through secure email by sending a request for the keys. or data owner send the secret key to personal domain user via secure email

Public Domain: The system defines role attributes, and a reader in a public domain obtains secret key from AAs, which binds the user to her claimed attributes/roles. In practice, there exist multiple AAs each governing a different subset of role attributes. AA in combine generates Global public parameter and attributes specific public and master parameter of their respective attributes using MA-ABE Setup discuss in next section. And publish public parameters with help of service provider. Two authorities Medical and Insurance are considered for this paper. Medical Authority monitors professional attributes for example “hospital, Doctor and Nurse Authority in combine generates the secret key for the public domain user of their claimed role attributes and send via secure email or in person public domain user has to obtain the secret key.

Encryption

The Patient Encrypt the medical records under a certain fine grained and role-based access policy for users from the Public domain to access, and under a selected set of data attributes that allows access from users in the Personal. And Uploads Encrypted File to the server.

View Medical Record File /Decryption

User from the personal or public domain can request the file form the server. Only user can view the records, provided the secret key policy matches with the at tributes attached with the files.

Revocations

Here we consider the revocation public domain users attributes. Revocation of user is similar to revocation of all attributes of the user. First the Attribute Authority redefines the MK and PK of the attributes of the revoked user and also generates re-encryption and re-secret keys for files and secrets key respectively then Attribute Authority sends the PRE keys for secret key to unrevoked user via secure email to public domain user and public domain user updates the secret key using re-secret Secret Keys and in last Authority re-encrypts the encrypted medical files stored on server using proxy re-encryption key generated in the first step.

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

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

CONCLUSION

In this Paper, we have presented the detail design and implementation detail of proposed a novel framework of secure sharing of personal medical records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their medical record files to allow fine-grained access. The framework addresses the unique challenges brought by multiple owners and users, in that we greatly reduce the complexity of key management while ensured the privacy. We utilize various forms of ABE to encrypt the medical record files, 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.

Acknowledgement

The authors would like to thank the ICET college authority and the guide for their valuable support. They would also like to thank the reviewers for their valuable feedback and suggestions.

REFERNCES

[1] 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

[2] 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

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

[4] 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.

[5] 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.

[6] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy Attribute-Based Encryption,” Proc. IEEE Symp. Security and Privacy (SP ’07), pp. 321-334, 2007.

[7] 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.

[8] Melissa Chase. Multi-authority Attribute Based Encryption. In TCC, volume 4392 of LNCS, pages 515–534. Springer 2007.

[9] 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.

[10] X. Liang, R. Lu, X. Lin, and X.S. Shen, “Ciphertext Policy Attribute Based Encryption with Efficient Revocation,” technical report, Univ. of Waterloo, 2010.

[11 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.