ISSN:0975-9646

Sharing of Personal Health Records Securely in Cloud Computing with Attribute Based Encryption

Muhib Anwar Lambay[1], M. Jhansi Lakshmi[2], Pralhad S. Gamare[3]

[1] PG Student, Department of CSE, [2] Associate Professor & HOD, Department of CSE,
[3] Assistant Professor, Department of Computer Engineering,
[1-2] Global Institute of Engineering and Technology, JNTU, Hyderabad, India.
[3] Rajendra Mane College of Engineering and Technology, Mumbai University, Maharashtra, *India.*

Abstract – **Personal Health Records (PHR) are important health fields to store health information of a person. These records are stored on untrusted servers which makes secure data sharing a challenging task. In Cloud computing the cloud servers are usually operated by third-party, which are almost certain to be outside the trust domain of cloud users. Initially the PHR access policies should be applied on these storage servers, also the confidentiality and security of sensitive data should be well protected against them. Various Encryption techniques are applied to carry out these tasks – encrypted PHR's are stored on storage servers while retaining secret key(s) to the data owner himself, user access is granted by issuing the corresponding data decryption keys. The main challenges for encryption techniques include simultaneously achieving system scalability and fine-grained data access control and efficient user/key management. To put forward these challenging tasks, various – Attribute-Based Encryption (ABE) techniques are used. Fine-grained data access control is guaranteed on untrusted servers.**

Keywords: **Personal Health Records (PHR), untrusted servers, Attribute-Based Encryption (ABE), Cloud Computing, fine-grained data access control.**

I Introduction

Personal Health Records/data information exchange is model for the sharing of personal medical records, which allows a person to create, manage and control his medical information in centralized place through the cloud. A Person can now share his medical records effectively with a wide variety of users such as family members, friends, consultants, doctors and insurance agencies.

The main concern is about the privacy of patients' PHR and who could gain access to the medical records when they are stored on untrusted servers. As patients lose full control to their own PHR, directly placing those sensitive data under the control of the untrusted servers cannot provide strong privacy assurance at all.

II Cloud Computing

Cloud Computing plays an important role by providing a facility of storage as service and software as service, by which software service providers can enjoy the virtually infinite and elastic storage and computing resources. While going for cloud storage, the data owner and cloud servers are in two different domains. On one hand, these untrusted servers are not entitled to access the outsourced data content for data secrecy, on the other hand, the data resources are not physically under the full control of data owner.

Storing PHR on the untrusted server leads to need of encryption mechanism to protect the PHR, before outsourcing to the cloud. To this end, the health records should be encrypted in addition to traditional access control mechanisms provided by the server. [1]

III Attribute Based Encryption

The concept of ABE was introduced along with another cryptography called fuzzy identity-based encryption (FIBE) [2] by Sahai and Waters. Both schemes are based on bilinear maps (pairing). An Attribute based encryption technique is used for encryption of PHR which provides a very good efficiency and security in storage, retrieval and sharing of PHR. In ABE system, users' private keys and ciphertext are characterized with sets of descriptive attributes and access policies respectively, and a specific key can decrypt exactly that ciphertext only if associated attributes and policy are matched.

A. Key-Policy Attribute-Based Encryption

The key-policy attribute-based encryption (KP-ABE) technique was first introduced in 2006 by Goyal et al. [3] In this encryption system, ciphertext are identified with sets of attributes. Private keys, on the other hand, are connected with access structures. A private key can decrypt only a ciphertext whose attributes set is an authorized set of the private key's access structure.

The KP-ABE is useful for providing the fine-grained access control to the PHR where it can efficiently specify that which part of PHR can be accessed by which user and what are the functions they can execute over there.

B. Multi-Authority Attribute-Based Encryption

The multi-authority attribute based encryption scheme is an advanced attribute based encryption in which it will have many attribute authority for handling the different set of users from various domains [1].

A user can select an attribute authority, provide some date to show that he is entitled to some of the attributes handled by that authority, and request for the decryption keys. The authority will process the user's request and run the attribute key generation algorithm, and finally provide the respective key to the user. A person can also opt to encrypt a message, in such case he uses the public parameters together with an attribute set of his choice to form the ciphertext. Any user who has decryption keys corresponding to the particular attribute set can use them for decryption.

In a PHR system the users will be from various domains like the consultants and doctors from health care centre and other users from insurance agencies. All these above users belong to the Public domain. Family and friends from personal relations belong to the Personal domain. So each user will be having different access control mechanism based on the relation with the patient or owner. Thus the MA-ABE technique will reduce the key-management issues and overhead to large extent and thus it will provide fine-grained access control to the system.

IV ADDITIONAL REQUIREMENTS

For access control of stored PHR, third party untrusted servers are considered. With cryptographic techniques, the aim is trying to find out who has access to which parts of a patient's PHR documents in a fine-grained manner.

A. *Symmetric key cryptography (SKC) based solutions:*

They are a class of algorithms for cryptography in which same cryptographic keys for both encryption of plaintext and decryption of ciphertext are being used. The keys may be identical or may be slightly different. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link Vimercati et.al.[4] Proposed a solution for securing outsourced data on semi-trusted servers based on symmetric key derivation methods, which can achieve fine-grained access control. But the involvement of file creation and user grant/revocation operations is linear to the number of authorized users, which is not much scalable.

B. *Public key cryptography (PKC) based solutions:*

PKC based solutions were proposed because of its ability to separate read and write privileges. To realize fine-grained access control, the traditional public key encryption (PKE) based schemes proposed by J. Benaloh, M. Chase, E. Horvitz, and K. Lauter [5] in their work "Patient controlled encryption: ensuring privacy of electronic medical records", they put forward how public and symmetric based encryption is used , disadvantage of their solution is either a key management is an overhead, or require encrypting multiple copies of a file using different users' keys.

C. *Attribute Based Encryption based solutions:*

The ABE technique is implemented to realize fine-grained access control for outsourced data; it is also used to secure electronic healthcare records (EHRs). Narayan et al. proposed an attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of Cipher Text-ABE (CP-ABE) [1]. But the ciphertext length increases gradually with the number of unrevoked users. In [16] a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs. Ibraimi et.al. [6] applied ciphertext policy ABE (CP-ABE)[18] to manage the sharing of PHRs, and introduced the concept of social/professional domains but they do not use multi-authority ABE . In [7], Akinyele et al. investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline. The drawback here is device dependency and user revocation is not supported. Also another drawback of all above solutions is problem of key-security as they consider single trusted authority.

V PROPOSED SOLUTION

Fig.1 shows the architecture of proposed system for sharing of the personal health records securely. The system is divided into two security domains i.e. Personal Domains (PSDs) and Public Domains (PUDs) as per the different users' data access requirements. The PUDs are composed of users whose access to PHR is based on their professional roles, such as medical researchers, doctors, consultants, nurses, and insurance agents. The PSD are composed of users who are personally connected with a data owner such as family members, relatives and close friends, they make access to PHR based on access rights assigned by the PHR owner. In PSD, the owner uses a key-policy attributed based encryption and generates secret key for his PSD users and in PUD the multi-authority attribute based encryption is used. Secret Key for PUD users is generated with the help of multiple attribute by the Attribute Authority in order to access the PHR.

In this system, the user accesses are managed by means of read and write access rights. The PHR-owner manages different access based on the attribute they defined. The on demand revocation of both the user and attribute are possible by this system. The policy updating is done by updating the attribute or access policy in the system. The emergency access is provided in the system by defining an emergency attribute in the system which provides break glass access. The system achieves data confidentiality by proving the enhanced MA-ABE technique. It also achieves the forward secrecy and security of write access control. Thus this system has benefits of fully-patient centric control over the PHR by the patient. It highly minimizes the key management overhead and it enhances the privacy guarantee.

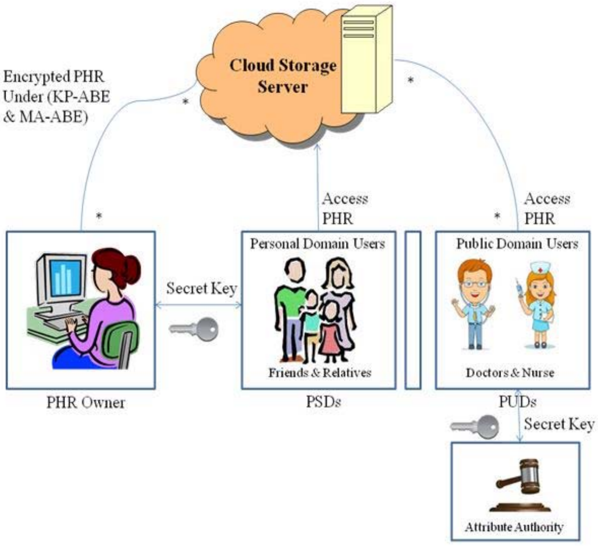

Fig.1 Architecture of Proposed System

VI Conclusion

The personal health records are now considered as the emerging trend in the personal health information exchange field. Here cloud server storage and sharing service is highly utilized by the users. The security of data is the main privacy issue and the attribute based encryptions and its related techniques are applied in order to enforce for the security purpose. In this paper several techniques of attribute based encryptions and its features are discussed. The PHR will use more secure encryption methods in the future for minimizing the key management problems and complexity and for providing more secure storage and sharing facility to the data's stored in the clouds servers.

References

[1]. S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010,pp. 47–52.

[2]. A. Sahai and B. Waters. Fuzzy identity-based encryption. Advances in Cryptology {EUROCRYPT 2005, pages 457{473, 2005.

[3]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06,2006, pp. 89–98.

[4]. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: management of access control evolution on outsourced data," in VLDB '07, 2007, pp. 123–134.

[5]. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, 2009, pp. 103–114.

[6]. 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.

[7]. 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 on mobile device. Technical report, Cryptology ePrint Archive, Report 2010/565, 2010. http://eprint.iacr.org/2010/565.