A STUDY ON CLOUD BASED SECURE PERSONAL HEALTH RECORD SHARING USING

BIRRU DEVENDER

Scholar, Shri Jagdishprasad
Jhabarmal Tibrewala University,
Jhunjhunu, India.

Dr. SYED ABDUL SATTAR

PhD (ECE), PhD (CS) Director
R&D, professor of ECE
Nawab shah Alam Khan College of
engineering & Technology,
New malakpet, malakpet,
Hyderabad. T.S. India.

ABSTRACT

A promising patient-centric model for health record exchange between multi users, Exchanging cloud-based patient health information holds huge guarantee for authorize patients and make sure more effective make public of patient health record. So in this manuscript, we design a novel system. It allows PHR owners to securely accumulate their health record on the semi-trusted cloud service providers, and to selectively share their health data with a wide range of PHR users. To reduce the key management complexity, we divide PHR users into two security domains named open domain and own domain. PHR owners encrypt their health data for the public realm using cipher text-policy attribute-based encryption scheme, while encrypt their health data for the personal domain using anonymous multi-receiver identity-based encryption scheme. Only authorized users whose credentials satisfy the specified cipher text-policy or whose identities belong to dedicated identities can decrypt the encrypted health data. Extensive analytical and experimental results are presented which show that our PHR system is secure, privacy-protected, scalable and efficient.

Keywords—*Personal health report, cloud computing, data isolation, fine-grained access control, attribute-based encryption*

INTRODCUTION:

In recent years, personal health record system has emerged as a patient-centric model of health information exchange. It enables the patient to create and control their health data in a centralized place through web-based application from anywhere and at any time, which has made the storage, Retrieval and sharing of the health data more efficient. Due to the high cost of building and maintaining specialized data centers, as well as vigorous development of cloud computing in recent years, many PHR services are outsourced to third-party cloud service providers (CSPs), for example, Microsoft Health Vault, Google Health, Indivo and MyPHR Although cloud-assisted PHR services could offer a great opportunity to improve the quality of health care services and potentially reduce health care costs, there have been wide privacy concerns as personal health information could be exposed to those semi-trusted CSPs and to unauthorized parties. Health data can reveal very sensitive information, including fertility, surgical procedures, emotional and psychological disorders and diseases, etc. There exist health care regulations such as HIPAA which is recently amended to incorporate business associates, but CSPs are usually not covered entities. Moreover,

due to the big value of health data, CSPs are often the targets of various malicious behaviors which may lead to exposure of health data. In addition, CSPs have significant commercial interest in collecting and sharing patients' health data with either pharmacy companies, research institutions or insurance companies. To keep sensitive health data confidential against those semi-trusted CSPs and unauthorized parties in a CB-PHR system, a natural way is to store only the encrypted data in the cloud. While it is important to allow patients to selectively share their health data with a wide range of users, including staffs from health care providers and medical research institutions, and family members or friends, thus it is essential to provide fine-grained data access control mechanisms that work with semi-trusted CSPs.

RELATED WORK:

Anonymous Multi-Receiver Identity-Based Encryption: Boneh and Franklin [1] proposed the first practical and secure identity-based encryption (IBE) scheme from bilinear pairings. Since then, IBE has attracted a lot of attention and a large number of IBE schemes and related systems have been proposed.

Considering a situation where a sender would like to encrypt a message for t receivers, the sender must encrypt the message t time using conventional IBE schemes. To improve the performance, Baek et al. [2] first introduced the notion of multi-receiver IBE scheme, and proposed an efficient provably secure multi-receiver IBE scheme from bilinear pairings. Next, Boyen and Waters [3] proposed an anonymous IBE scheme to guarantee receiver's privacy, where the cipher text does not leak the identity of the recipient. Later, Fan et al. [4] introduced the concept of anonymous multi-receiver IBE (AMRIBE) scheme, an proposed an AMRIBE scheme from bilinear parings. Fan et al. claimed that their AMRIBE scheme makes it impossible for an attacker or any other receiver to derive the identity of a message receiver such that the privacy of every receiver can be guaranteed. Unfortunately, Chien [5] showed that in Fan et al.'s AMRIBE scheme any selected receiver may extract the identities of the other selected receivers, and presented an improved AMRIBE scheme. However, only heuristic arguments for security proofs are presented. Recently, Tseng et al. [6] proposed an efficient AMRIBE scheme with complete receiver anonymity and proved that the scheme is semantically secure against adaptively chosen-cipher text attacks. Attribute-Based Encryption: In some scenarios, the recipient of the cipher text is not yet known at the time of the encryption or there is more than one recipient who should be able to decrypt the cipher text. To preserve data confidentiality and enforce fine-grained access control simultaneously, Sahai and Waters [7] first introduced the concept of attribute-based encryption (ABE), which is envisioned as an important tool for addressing the problem of secure and fine-grained data sharing and access control.

ABE has attracted lots of attention from both academia and industry in recent years, various ABE schemes have been proposed, such as [8–13]. There are two main types of ABE schemes in the literatures: Key-Policy

ABE (KPABE) and Cipher text-Policy ABE (CP-ABE).

In a KP-ABE system, cipher texts are labeled by the sender with a set of descriptive attributes, and users' private keys are issued by the trusted attribute authority are associated with access structures that specify which type of cipher texts the key can decrypt.

Goyal et al. [8] proposed the first KP-ABE scheme, which was very expressive in that it allowed the access policies to be expressed by any monotonic formula over encrypted data. While in a CP-ABE system, when a sender encrypts a message, they specify a specific access policy in terms of access structure over attributes in the cipher text, stating what kind of receivers will be able to decrypt the cipher text. Users possess sets of attributes and obtain corresponding secret attribute keys from the attribute authority; such a user can decrypt a cipher text if his/her attributes satisfy the access policy associated with the cipher text. Bethen court et al. [9]constructed the first CP-ABE scheme, but its security was proved in the generic group model.

Later, Waters [10] proposed an efficient CP-ABE scheme with expressive access policy described in general linear secret sharing scheme. Several CB-PHR systems using ABE schemes have been developed in recent years. Ibraimi et al. [14] propose a secure PHR management system using Betten court et al.'s CP-ABE scheme, which allows PHR owners to encrypt their health data according to an access policy over a set of attributes issued by two trusted authorities.

Later, Li et al. [15] proposed a secure and scalable PHR sharing framework on semi-trusted storage servers under multi owner settings by leveraging both KP-ABE and CP-ABE techniques.

PROBLEM DEFINATION

Here we tend to attempt to study a PHR system wherever there ar various PHR house owners and PHR users. The house owners may be patients World Health Organization have full access management over their own PHR knowledge wherever they will construct/generate, maintains and delete it. There's a server that belongs to the PHR service supplier that stores all the owners' PHRs. The users might come back from numerous fields; as an example say an acquaintance, a guardian or a investigator. Here users attempt to access the PHR records through the server to scan or write to someone's PHR, and at a similar time users have right to access to multiple owners' knowledge. Following ar the three phases:

A. Unauthorized Users Access: it's a vital demand for economical PHR access is to modify "patient-centric" sharing. This suggests that the patient ought to have all the management over their personal health record. They will verify that users shall have access to their case history. User controlled scan write access and revocation is that the 2 main security objectives or issues for any electronic health record model. User management led write access control in PHR system states the bar of unauthorized users to access the records and modifying it.

B. Fine Grained Access management Fine grained access management ought to be employed in a way that totally different completely different users are approved to scan different sets of documents. The most

objective of our model is to grant secure patient-centric PHR access and economical key management at the same time. Whenever a user's attribute isn't any longer applicable, the user needn't be ready to access additional PHR files victimization that very same attribute.

C. Attribute Revocation the PHR system ought to permit users from each the private domain and property right. Considering the teams of finish users from the general public domain is also Brooding angina in size and unsure, the system ought to be ascendible, in managing the quality in key management, communication, computation and storage too. Also, the owners' struggle in governing users and keys ought to be reduced to get pleasure from usability.

Cloud Data Storage

Cloud storage is the flexible method of storage in which data can be securely stored as use on pay nature. Data stored in the cloud is made secure by cryptographic methods. Cloud allows anywhere access of stored data. Characteristics of secure cloud data storage are Integrity, Availability and Confidentiality. Advantages of cloud storage over traditional server are

- Flexible data access.
- Secure data storage.
- High availability.
- Enhanced sharing

Sharing is an area of ongoing researches in cloud computing. Sharing can be done by various methods. One of the popular methods is to share keys using Diffie-Hellman key exchange method. This shared key can be used to share the data. In a distributed and dynamic scenario this method becomes inadequate. Re-encryption is another method used in data sharing.

Re-encryption

Re-encryption is the process of modifying cipher text encrypted under sender's key to a different cipher text under recipient's public key. In this process security is maintained only if plain text is not encountered during the re-encryption operation.Blinding process in the encryption does further enhancing of security. Various re-encryption schemes are discussed below.

CONCLUSION

In this paper regarding problem statement of data sharing schemes have been analyzed and compared. Some methods provide better protection against replay attacks [5] without perfect clock synchronization. But it has a disadvantage of handling large number of keys. [1] Provide better sharing of data using less number of per user keys and resist attacks by key sharing methods. Fine grained access control is provided in [3], [5]. Asymmetric proxy re-encryption methods [12], [14] and [17] are also compared.

REFERENCES

[1] D. Boneh and M. Franklin (2001) Identity-based encryption from theWeil pairing, CRYPTO 2001, LNCS 2139, Springer Berlin Heidelberg, pp. 213–229.

[2] J. Baek, R. Safavi-Naini and W. Susilo (2005) Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption, PKC 2005, LNCS 3386, Springer Berlin Heidelberg, pp.380– 397.

[3] X. Boyen and B. Waters (2006) Anonymous hierarchical identity-based encryption (without random oracles), CRYPTO 2006, LNCS 4117, Springer Berlin Heidelberg, pp. 290–307.

[4] C.I. Fan, L.Y. Huang and P.H. Ho (2010) Anonymous multireceiver identity-based encryption,

IEEE Transactions on Computers, Vol. 59, No. 9, pp. 1239–1249.

[5] H.Y. Chien (2012) Improved anonymous multireceiver identity-based encryption, The Computer Journal, Vol. 55, No. 4, pp. 439–445.

[6] Y.M. Tseng, Y.H. Huang and H.J. Chang (2012) CCA-secure anonymous multi-receiver ID-based encryption, 26th International Conference on Advanced Information Networking and Applications Workshops, IEEE, pp. 177–182.

[7] A. Sahai and b. Waters (2005) Fuzzy identitybased encryption, EUROCRYPT 2005, LNCS 3494,

Springer Berlin Heidelberg, pp. 457–473.

[8] V. Goyal, O. Pandey, A. Sahai and B. Waters (2006) Attribute-based encryption for fine-grained access control of encrypted data, CCS 2006, ACM, New York, pp. 89–98.

[9] J. Bethencourt, A. Sahai and B. Waters (2007) Ciphertext-policy attribute-based encryption, IEEE Symposium on Security and Privacy, IEEE, pp. 321–334.

[10] B. Waters (2011) Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization, PKC 2011, LNCS 6571, Springer Berlin Heidelberg, pp. 53–70.

[11] J. Li, Q. Wang, C. Wang and R. Kui (2011) Enhancing attribute-based encryption with attribute hierarchy,Mobile Network Application, Vol. 16, No. 5, pp. 553–561.

[12] C.J.Wang and J.F. Luo (2013) An efficient key-policy attribute-based encryption scheme with constant ciphertext length, Mathematical Problems in Engineering, Hindawi, Vol. 2013, pp. 1–7.

[13] J. Li, X.Y. Huang, J.W. Li, X.F. Chen and Y. Xiang (2014) Securely outsourcing attribute-based encryption with checkability, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 8, pp. 2201– 2210.

[14] L. Ibraimi, M. Asim and M. Petkovic (2009) Secure management of personal health records by applying attribute-based encryption, 6th International Workshop on Wearable Micro and Nano Technologies for Personalized Health (pHealth), IEEE, pp. 71–74.

[15] M. Li, S.C. Yu, Y. Zheng, K. Ren andW.J. Lou (2013) Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 1, pp. 131–143.

[16] T. Okamoto and D. Pointcheval (2001) REACT: rapid enhanced-security asymmetric cryptosystem transform, CT-RSA 2001, LNCS 2020, Springer Berlin Heidelberg, pp. 159–174.

[17] E. Fujisaki and T. Okamoto (2011) Secure integration of asymmetric and symmetric encryption schemes, Journal of Cryptology, Vol. 26, No. 1, pp. 80–101.

[18] A. Beimel (1996) Secure schemes for secret sharing and key distribution, PhD Thesis, Israel Institute of Technology, Technion, Haifa, Israel.

[19] J.A. Akinyele, et al. (2013) Charm: a framework for rapidly prototyping cryptosystems, Journal of Cryptographic Engineering, Vol. 3, No. 2, pp. 111-128.

[20] M. Green and J.A. Akinyele (2014) The functional encryption library, Online, accessed 18-July-2014, http://code.google.com/p/libfenc/.

[21] E. Young and T. Hudson (2014) The openssl project, Online, accessed 18-July-2014, http:// www.openssl.org/.

[22] B.Lynn (2014) The pairing-based cryptography library, Online, accessed 18-July-2014, http:// crypto.stanford.edu/pbc/.