International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 1, January - 2014

Security of Personal Health Records through Attribute Based Encryption in Cloud Computing

Snehal Pise
PG Student,
Department of Computer Engineering,
Sinhgad Technical Education Society's, Smt.
KashibaiNavale college of Engineering,
Pune, Maharashtra, India

Pramod Mali
AssistantProfessor,
Department of Computer Engineering,
Sinhgad Technical Education Society's, Smt.
KashibaiNavale college of Engineering,
Pune, Maharashtra, India

Abstract

Now-a-days sensitive data like PHRs are stored on third-party server such as cloud.Recently, PHR system is evolved as a patient-centric model of health information exchange. In order to reduce the operational cost of specialized data centres and to use elastic resources of cloud, the PHR service providers are shifting their PHR application services into the cloud.

To secure PHRs and to achieve fine grained access control, new technique of public-cryptosystem called as Attribute Based Encryption (ABE) is used. Various issues like scalability, key management, and efficient user revocation are handled in proposed system. The main focus is given on multi-owner and multi-authority scenario. The users in the system are divided into public and private domains.

Proposed system enables dynamic modification of access policies or file attributes. In emergency scenario, break-glass access is provided. It supports on-demand revocation of user or attribute. Proposed system is robust in terms of security, scalability and efficiency.

Keywords: Cloud Computing, Attribute Based Encryption, PHR

1. Introduction

Recently, PHR is considered as a patient-centric model of health information exchange. It facilitates the patient to create and manage her/his own personal health information (PHI) in one centralized place through the web. It enables storing, retrieval and sharing of medical information in an efficient way [1]. PHRs contain a diverse range of data like- allergies, chronic diseases, family history, illness, imaging reports, hospitalizations, surgeries, vaccinations etc. PHR system allows patient to merge potentially separate health records from multiple geographically dispersed health providers into one centralized profile over passage of time. So it is possible for the users, like medical practitioners, researchers, family members and friends to gain access to and utilize one's PHR on demand according to their need, therefore making the healthcare processes much more efficient and accurate.

Now-a-days PHR service providers are shifting their PHR storage and applications into the cloud in order to utilize storage facilities provided by the cloud [3]. Cloud computing reduces the operational cost of building and maintaining the specialized data centres for PHR system. For example, Microsoft Health Vault is cloud platform provider.

Though cloud computing has provided virtually infinite storage and large computation resources, it is facing many data security and privacy challenges which may impede its wide adoption. Privacy of patient's personal health data and who could have access to PHRs stored in cloud server is a main challenge. As sensitive PHRs are under the control of the servers which are operated by commercial providers, there is a possibility of leaking the data by misbehaviour of insider in the system. 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 [3]. Though health care regulations like Health Insurance Portability and Accountability Act of 1996 (HIPAA) exists, confidentiality of PHRs is not assured.

To deal with the data security, privacy and confidentiality issues, encryption of PHRs is a promising approach. PHR owners should have full control over the selective sharing of their own PHR data and able to decide which users have access to which part of their PHR. As there are multiple users who want to access the record for different purposes, the record must be accessed at fine grained level. There are various techniques to encrypt the PHRs – symmetric key encryption, public key encryption etc. By applying these techniques records are shared at coarse-grained level and issues like key management, scalability are not resolved.

New cryptographic approach is introduced to achieve fine-grained sharing of encrypted data that is called as Attribute Based Encryption (ABE).

2. Motivation

In the proposed system, a patient-centric secure data framework for cloud based PHR is proposed. There are several common drawbacks of the previous works:

- Use of a single Trusted Authority(TA) in the system which creates a load bottleneck
- Most of the existing work is not applicable to multiple data owners and users
- Do not differentiate between private and public domains
- Lack of on-demand user revocation and dynamic policy updates

The proposed system is motivated to remove all the drawbacks of the previousworks. The main contributions added to the proposed system are:

- Secure sharing of PHRs in cloud computing under multi-owner settings
- Key management issues are handled by dividing users of the system into public and private domains
- Minimal key management overhead for both owner and users in the system
- Use of Multi-Authority Attribute Based Encryption (MA-ABE) to improve the security in public domain
- Write access control, on-demand revocation of attribute or user, break glass access to the PHRs under emergency scenarios are efficiently handled

3. Related Work

To secure sensitive data on the cloud and to achieve fine-grained access control various techniques of cryptography are used which include symmetric key cryptography, public key cryptography and attribute based cryptography. In symmetric key cryptography, identical keys are used for both encryption of plain text and decryption of cipher text. If keys are not identical then there is a simple transformation to go between the two keys. A shared secretes between two or more parties is represented by the keys that can be used to maintain a private information link. A solution for securing outsourced data on semi-trusted servers based on symmetric key cryptography method is proposed in [11]. As user grant or revocation operations are linear to the number of users, this system is less scalable.

In public key cryptography, two different keys are used for encryption and decryption. In [8], use of public key cryptography is used to achieve fine-grained access control. This scheme leads to the high key management overhead and it requires encrypting multiple copies of a file using different users' keys.

An Identity Based Encryption scheme is proposed in [9] which are known as Fuzzy Identity Based Encryption. Here an identity is viewed as set of descriptive attributes. In this scheme, a user with the secrete key for the identity ω is allowed to decrypt a cipher text encrypted with the public key ώ if and only if ω and ώ are close to each other measured by the "set overlap" distance metric. Certain amount of error-tolerance in the identities can be allowed in this system. It is useful for two applications. The first is for Identity Based Encryption that uses biometric identities. This scheme views user's biometric as that user's identity which is described by several attributes and then encrypt to the user using their biometric identity. The error-tolerance property of Fuzzy-IBE allows for a private key (derived from a measurement of a biometric) to decrypt a cipher text encrypted with a slightly different measurement of the same biometric.Second application is "attribute-based encryption". In this application a party will wish to encrypt a document to all users that have a certain set of attributes. Any user who has an identity that contains all of these attributes could decrypt the document. The advantage of using Fuzzy IBE is that the document can be stored on simple untrusted storage server instead of relying on trusted server to perform authentication checks before delivering a document.

In an ABE, a user's key and cipher text are labelled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key. New method of Attribute Based Encryption is proposed that is called as Key-Policy Attribute Based Encryption [12]. This scheme allows fine-grained sharing of encrypted data. Fine-grained access control system facilitates granting differential access rights to a set of users and allows flexibility in specifying the access rights of individual users. In KP-ABE, each cipher text is labeled by set of descriptive attributes and each private key associated with an access structure. Access structure specifies which type of cipher text the key can decrypt. If user satisfies the key's access structure with attribute associated with cipher text then she/he is allowed to decrypt that record related to that cipher text. Since the access structure is defined in private key itself it is called as Key-Policy Attribute Based Encryption. Here single data owner or patient is a Trusted Authority (TA). User revocation rights are given to data owner. Data owner can revoke the user by delegating the updates of affected cipher texts and users secrete keys to the cloud server. But, this scheme is not applicable to the PHR system with multiple data owners.

Another method of Attribute Based Encryption is introduced called as Ciphertext-Policy Attribute Based Encryption [6][10]. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in this system attributes are used to describe a user's credentials and a party encrypting data determines a policy for who can decrypt. A user's private key will be associated with an arbitrary number of attributes expressed as strings. On the other hand, when a party encrypts a message, they specify an associated access structure over attributes. A user will only be able to decrypt a ciphertext if that user's attributes pass through the ciphertext's access structure. At a mathematical level, access structures are described by a monotonic “access tree”, where nodes of the access structure are composed of threshold gates and the leaves describe attributes.

In [1], advantages of KP-ABE and CP-ABE are combined together to introduce new Attribute Based Encryption method. Here focus is on the multiple data owner scenario. Users are divided into two types of domains - personal and public domains. Users in public domain are managed by multiple authorities by applying multi-authority ABE (MA-ABE) and users in personal domain are managed by data owner itself. In this way minimal key management overhead is incurred for both owners and users in the system. Write access control, dynamic policy updates and break-glass access issues are handled in very efficient manner.

4. Proposed Work

Aim of the proposed work is to provide a novel patient-centric secure data sharing framework for cloud-based PHR systems. A PHR system with multiple PHR owners and PHR users is considered. Owners are patients who can create, manage and delete the PHR data. Patients have full control over their own PHR data. To encrypt each patient's PHR file an Attribute Based Encryption (ABE) technique is used to achieve fine-grained and scalable data access control for PHRs. All the encrypted PHRs are stored on cloud server.

Users are divided into Public Domains (PUDs) and Private Domains (PSDs). The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers etc. Users from the PSDs are personally associated with a data owner e.g. family members or close friends, and they make access to PHRs based on access rights assigned by the owner. Each user will be given corresponding secrete and attribute key. Based on the attributes and the given keys user can view PHR documents in order to read or write to someone's PHR.

In case of emergency scenario, user can issue an emergency key from the emergency department and access the corresponding PHR. Proposed system enables the dynamic modification of file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenario.

5. Conclusion

The proposed PHR system ensures the secure sharing of Personal Health Records at fine grained access level. Large number of users from public and private domain can access the records efficiently. Main focus isgiven on scalability and security of the system. Patients have complete control of their own privacy through encrypting their PHR files using attribute-based encryption. In proposed framework, the challenges brought by multiple owners and users are addressed. This framework greatly reduces the complexity of key management while enhances the privacy guarantee compared with previous work. The framework enhances the existing MA-ABE scheme to handle efficient and on-demand user revocation, and proves its security.

6. References

[1] Ming Li,Shucheng Yu,Yao Zheng,KuiRen,and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption",in IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, JANUARY 2013, VOL. 24, NO. 1.

[2] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing", in ICDCS'11, Jun.2011.

[3] M. Li, S. Yu, K. Ren, and W. Lou, “Securing Personal HealthRecords in Cloud Computing: Patient-Centric and Fine-GrainedData Access Control in Multi-Owner Settings,” Proc. Sixth Int’lICST Conf. Security and Privacy in Comm. Networks (SecureComm ’10), Sept. 2010, pp. 89-106.

[4] H. Lohr, A. R. Sadeghi, and M. Winandy, "Securing the e-health cloud", in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI'10,2010, pp.220-229.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-graineddata access control in cloud computing", in IEEE INFOCOM'10, 2010.

[6] X. Liang, R. Lu, X. Lin, and S. Shen, "Ciphertext policy attribute based encryption with efficient revocation", Technical Report, University of Waterloo, 2010.

[7] M. Chase and S. S. Chow, "Improving privacy and security in multi-authorityattribute-based encryption", in CCS'09, 2009, pp.121-130.

[8] 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.

[9] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficientrevocation", in ACM CCS, ser. CCS '08, 2008, pp.417-426.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute based encryption", in IEEE SG P'07, 2007, pp.321-334.

[11] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, “Over-encryption: management of access control evolution onoutsourced data,” in VLDB ’07, 2007, pp. 123–134.

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