ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Attribute-Based Encryption on Personal Health Records (PHR) in Cloud Computing

K. Srujana
M.Tech,
Department of CSE,
AVNIET, JNTUH, Hyderabad.

SK Abdul Nabi
Professor and HOD,
Department of CSE,
AVNIET, JNTUH, Hyderabad.

Abstract:

This paper presents the design and implementation of Personal Health Records and providing security to them while they are stored at third party such as cloud. Personal Health Record is web based application that allows people to access and co-ordinate their lifelong health information. The patient have control over access to their own PHR. To achieve security of personal health records we use the attribute based encryption to encrypt the data before outsourcing it.

Here we focus on multiple types of PHR owner scenario and division of personal health records users into multiple security domains which reduce key management complexity for owners and users. A high degree of patient's privacy is guaranteed. Our scheme gives personal health record owner full control of his/her data. Extensive security and performance analysis shows that the proposed scheme is highly efficient.

Keywords:

Servers, Encryption, Access control, Medical services, Scalability, attribute-based encryption, Personal health records, cloud computing, data privacy, fine-grained access control.

INTRODUCTION:

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. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method 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. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file.

Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

LITERATURE SURVEY:

This paper is mostly related to works in cryptographicily enforced access control for outsourced data and attribute based encryption. To realize fine-grained access control, the traditional public key encryption (PKE) based schemes either incur high key managemen overhead, or require encrypting multiple copies of a file using different users keys. To improve upon the scalability of the above solutions, one-to-many encrypt ion methods such as ABE can be used. In Goya let. alls seminal paper on ABE data is encrypted under a set of attributes so that multiple users who possess proper keys can decrypt.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

This potentially makes encryption and key management more efficient. Fundamental property of ABE is preventing against user collusion. In addition, the encrypt or is not required to know the ACL. ABE for Fine-grained Data Access Control:- A number of works used ABE to realize fine-grained access control for outsourced data [9]. Especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs).Recently, Narayan et al. proposed an attribute-based infrastructure for EHR systems, where each patients EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of unrevoked users.

In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs. Ibraimi et.al . applied ciphertext policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/ professional domains. In , Akinyele et al. investigated using ABE to gen-erate self-protecting EMRs, which can either be stored on cloud servers or cellphones so that EMR could be accessed when the health provider is offline. However, there are several common drawbacks of the above works. First, they usually assume the use of a single trusted authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem since the TA can access all the encrypted files, opening the door for potential privacy exposure.

In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users attributes or roles and generating secret keys. In fact, different organizations usually form their own (sub) domains and become suitable authorities to define and certify different sets of attributes belonging to their (sub)domains (i.e., divide and rule). For example, a professional association would be responsible for certifying medical specialties, while a regional health provider would certify the job ranks of its staffs. Second, there still lacks an efficient and on-demand user revocation mechanism for ABE with the support for dynamic policy updates/changes, which are essential parts of secure PHR sharing. Finally, most of the existing works do not differentiate between the personal and public do-mains, which have different attribute dentitions, key management requirements and scalability issues.

Our idea of conceptually dividing the system into two types of domains is similar with that in, however a key difference is in a single TA is still assumed to govern the whole professional domain. Recently, Yu et al . (YWRL) applied key-policy ABE to secure outsourced data in the cloud where a single data owner can encrypt her data and share with multiple authorized users, by distributing keys to them that contain attribute-based access privileges. They also propose a method for the data owner to revoke a user efficiently by delegating the updates of affected ciphertexts and user secret keys to the cloud server. Since the key update operations can be aggregated over time, their scheme achieves low amortized overhead. However, in the YWRL scheme, the data owner is also a TA at the same time.

It would be inefficient to be applied to a PHR system with multiple data owners and users, because then each user would receive many keys from multiple owners, even if the keys contain the same sets of attributes. On the other hand, Chase and Chow proposed a multiple-authority ABE (CC MA-ABE) solution in which multiple TAs, each governing a different subset of the systems users attributes, generate user secret keys collectively. A user needs to obtain one part of her key from each TA. This scheme prevents against collusion among at most N – 2 TAs, in addition to user collusion resistance. However, it is not clear how to realize efficient user revocation. In addition, since CC MA-ABE embeds the access policy in users keys rather than the ciphertext, a direct application of it to a PHR system is non-intuitive, as it is not clear how to allow data owners to specify their file access policies.

PROBLEMS IN CURRENT SYSTEM:

Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft Health Vault. While it is exciting to have convenient 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. There have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. They usually assume the use of a single trusted authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem since the TA can access all the encrypted files, opening the door for potential privacy exposure. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys.

PROPOSED SYSTEM:

To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file.We endeavor to study the patient centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved.

ARCHITECTURE:

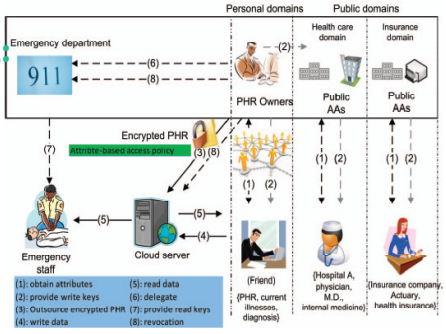


Fig. 1. The proposed framework for patient-centric, secure and scalable PHR sharing on semi-trusted storage under multi-owner settings.

RELATED WORK:

Key-Policy Attribute-based Encryption (KP-ABE):

KP-ABE is a crypto system for fine grained sharing of encrypted data. In KP-ABE cipher text are label with attributes and private key are associated with access structures that control which cipher text a user is able to decrypt. It is used for securing sensitive information stored by third parties on the internet.

Cipher text Policy Attribute based Encryption (CP-ABE):

CP-ABE is a policy to acquire complex control on encrypted data. This technique is used to keep encrypted data confidential.

Encryption (MA-ABE):

MA-ABE method allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k.

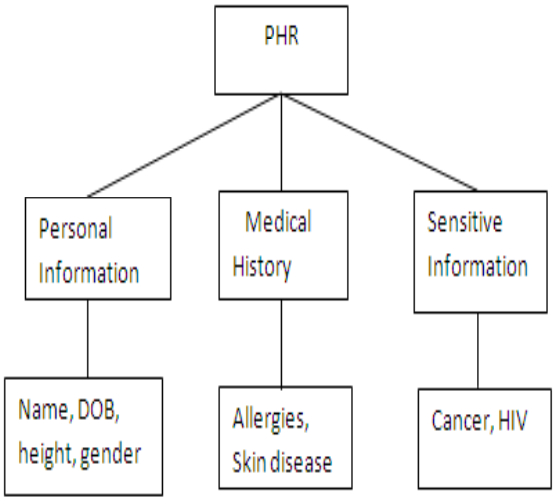
ATTRIBUTE BASED ENCRYPTION:

Using attribute based encryption technique we are providing security to the database. A sensitive data is shared and stored on cloud server, there will be a need to encrypt data stored at third party. In Attribute based encryption cipher text labeled with set of attribute. Private key associated with access structure that control which cipher text a user is able to decrypt.

We are using attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of the users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-retrieval to solve, and remain largely open up-to-date. THE ATTRIBUTE HIERARCHY :-We are using attribute based encryption for providing security. For that we use following distribution of attributes that are mainly important.



METHODOLOGY:

Registration:

Normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files – leaf nodes is atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader have access to. Two ABE systems are involved: for each PSD the revocable KP-ABE scheme is adopted for each PUD, our proposed revocable MA-ABE scheme.

- PUD - public domains
- PSD - personal domains
- AA - attribute authority
- MA-ABE - multi-authority ABE
- KP-ABE - key policy ABE

UPLOAD FILES:

Users upload their files with secure key probabilities. The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file encrypted both under a certain fine grained model.

ABE for Fine-grained Data Access Control:

ABE to realize fine-grained access control for outsourced data especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). An attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation.

However, the cipher text length grows linearly with the number of un revoked users. In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs applied cipher text policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains 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.

Setup and Key Distribution:

The system first defines a common universe of data attributes shared by every PSD, such as "basic profile", "medical history", "allergies", and "prescriptions". An emergency attribute is also defined for break-glass access. Each PHR owner's client application generates its corresponding public/master keys. The public keys can be published via user's profile in an online healthcare social-network (HSN)

There are two ways for distributing secret keys.

» First, when first using the PHR service, a PHR owner can specify the access privilege of a data reader in her PSD, and let her application generate and distribute corresponding key to the latter, in a way resembling invitations in GoogleDoc.

» Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access) to the PHR owner via HSN, and the owner will grant her a subset of requested data types. Based on that, the policy engine of the application automatically derives an access structure, and runs keygen of KP-ABE to generate the user secret key that embeds her access structure.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Break-glass module:

In this module when an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR. In our framework, each owner's PHR's access right is also delegated to an emergency department ED to prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED.

Data confidentiality:

Attribute Based Encryption- encrypted PHR files are upload to the server by the owners. Every owner's PHR file is ciphered both under a certain role-based and fine grained access policy for users from the public domain to access and under a chosen group of data attributes that allows access from users in the personal domain. The PHR files can be decrypt by the authoritative users, excluding the server.

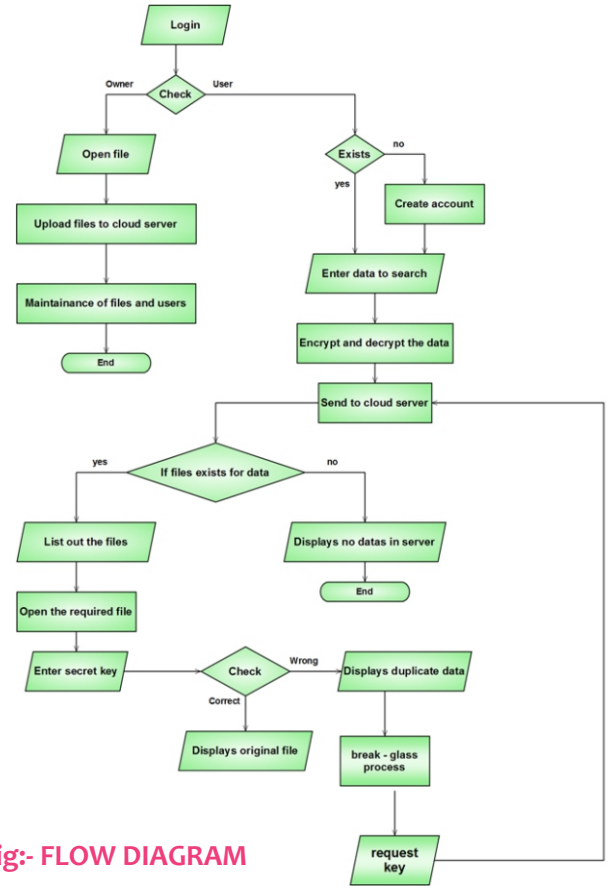


Fig:- FLOW DIAGRAM

CONCLUSION:

In this paper we have proposed a novel structure of secure distribution of Personal Health Records in cloud computing in this paper. Taking into consideration moderately responsible cloud servers, we dispute that to completely apprehend the patient-centric model, patients shall have extensive manage of their own privacy through enciphering their Personal Health Record files to permit fine-grained access. The method addresses the distinctive goals brought by various Personal Health Record users and owners, in that we completely decrease the complication of key management while enhance the privacy assurance compared with prior works. We use Attribute Based Encryption to encipher the Personal Health Record data, hence that patients can permit access not only by personal users, but also many users from public domains with different professional roles, affiliations and qualifications. In addition, we enhance an existing Multi Authority Attribute Based Encryption scheme to manage on-demand user revocation, efficient, and prove its security.

References:

1. Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee,G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M.: Above the clouds: A Berkeley view of cloud computing (February 2009).

2. At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded (2006), http://articles.latimes.com/2006/jun/26/health/he-privacy26.

3. The health insurance portability and accountability act of 1996 (1996), http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp.

4. Benaloh, J., Chase, M., Horvitz, E., Lauter, K.: Patient controlled encryption: ensuring privacy of electronic medical records. In: CCSW 2009: Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 103–114 (2009).

5. Mandl, K.D., Szolovits, P., Kohane, I.S.: Public standards and patients' control: how to keep electronic medical records accessible but private. BMJ 322(7281), 283 (2001)

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

6. Wang,W., Li, Z., Owens, R., Bhargava, B.: Secure and efficient access to outsourced data. In: CCSW 2009, pp. 55–66 (2009)

7. Damiani, E., di Vimercati, S.D.C., Foresti, S., Jajodia, S., Paraboschi, S., Samarati, P.: Key management for multi-user encrypted databases. In: StorageSS 2005, pp. 74–83 (2005)

8. Atallah, M.J., Frikken, K.B., Blanton, M.: Dynamic and efficient key management for access hierarchies. In: CCS 2005, pp. 190–202 (2005)

9. Blundo, C., Cimato, S., De Capitani di Vimercati, S., De Santis, A., Foresti, S., Paraboschi, S., Samarati, P.: Managing key hierarchies for access control enforcement: Heuristic approaches. In: Computers & Security (2010) (to appear)

10. Scholl, M., Stine, K., Lin, K., Steinberg, D.: Draft security architecture design process for health information exchanges (HIEs). Report, NIST (2009)

11. Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R.: Proposed NIST standard for role-based access control. ACM TISSEC 4(3), 224–274 (2001)

12. Jin, J., Ahn, G.-J., Hu, H., Covington, M.J., Zhang, X.: Patient-centric authorization framework for sharing electronic health records. In: SACMAT 2009, pp. 125–134 (2009)

13. di Vimercati, S.D.C., Foresti, S., Jajodia, S., Paraboschi, S., Samarati, P.: Overencryption: management of access control evolution on outsourced data. In: VLDB 2007, pp. 123–134 (2007)

14. Dong, C., Russello, G., Dulay, N.: Shared and searchable encrypted data for untrusted servers. In: DBSec 2008, pp. 127–143 (2008)

15. Li, M., Lou,W., Ren, K.: Data security and privacy in wireless body area networks. IEEE Wireless Communications Magazine (February 2010)

16. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for finegrained access control of encrypted data. In: CCS 2006, pp. 89–98 (2006)

17. Boldyreva, A., Goyal, V., Kumar, V.: Identity-based encryption with efficient revocation. In: CCS 2008, pp. 417–426 (2008)

18. Ibraimi, L., Petkovic, M., Nikova, S., Hartel, P., Jonker, W.: Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes (2009), http://purl.org/utwente/65471

19. Yu, S., Wang, C., Ren, K., Lou, W.: Achieving secure, scalable, and fine-grained data access control in cloud computing. In: IEEE INFOCOM 2010 (2010)

20. Yu, S., Wang, C., Ren, K., Lou, W.: Attribute based data sharing with attribute revocation. In: ASIACCS 2010 (2010)

21. Liang, X., Lu, R., Lin, X., Shen, X.S.: Patient self-controllable access policy on phi in ehealthcare systems. In: AHIC 2010 (2010)

22. Ibraimi, L., Asim, M., Petkovic, M.: Secure management of personal health records by applying attribute-based encryption. Technical Report, University of Twente (2009)

23. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE S& P 2007, pp. 321–334 (2007)

24. Chase, M., Chow, S.S.: Improving privacy and security in multi-authority attributebased encryption. In: CCS 2009, pp. 121–130 (2009)

25. Liang, X., Lu, R., Lin, X., Shen, X.S.: Ciphertext policy attribute based encryption with efficient revocation. Technical Report, University of Waterloo (2010)