International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 3, Issue 4, July-August 2014 ISSN 2278-6856

Securing Personal Health Records in Cloud Server

T. Baba[1], K. Jeevan Pradeep[2]

[1]Dept of CSE, Sree Vidyanikethan Engineering College,
Tirupati, India

[2] Dept of CSE, Sree Vidyanikethan Engineering College,
Tirupati, India

Abstract

Personal health record (PHR) service is an emerging model for health information exchange. It allows patients to create, manage, control and share their health information with other users as well as healthcare providers. In reality, a PHR service is likely to be hosted by third-party cloud service providers in order to enhance its interoperability. However, there have been serious privacy concerns about outsourcing patients' PHR data to cloud servers, not only because cloud providers are generally not covered entities under Health Insurance Portability and Accountability Act (HIPAA), but also due to an increasing number of cloud data breach incidents happened in recent years. In this paper we concentrate on multiple scenario of PHR owner and division of PHR users into multiple security domains which diminish key management complication for both PHR owners and users. An elevated scale of patient's privacy is guaranteed. Our scheme provides personal health record owner full control of his/her data. Extensive performance along with security analysis shows that the proposed scheme is highly capable.

Keywords: Personal Health Records (PHR), Attribute based encryption, Cloud servers, Security.

1. INTRODUCTION

The term personal health record (PHR) has undergone substantial changes along with the emergence of cloud computing. A PHR could be a set of computer-based tools that enable people to access and also synchronize their lifelong health information as well as to make suitable components of it accessible to those who want it. Most healthcare information technology vendors as well as healthcare providers started their PHR services as a simple storage service, and then turn them into a complicated social-network like service for patients to share personal health information with others. Therefore, by the existence of cloud computing into PHR service, several important issues regarding PHR solitude as well as security require enhanced evaluation. Potentially, PHR could protect patient solitude as well as security in many ways that are more secured than conventional paper based patient records, since it can provide additional security feature such as password protecting and audit tracking.

Research Goals

The fundamental goal of this paper is to propose and implement a practical design to achieve fine-grained data access control of PHR data in a semi-trusted cloud computing environments. We demonstrate PHR privacy issue can be partially solved by reducing it to the underlying cryptographic and key management problem. Relying on the novel one-to-many cryptography scheme, such as attribute-based encryption (ABE), we wish to construct a PHR architecture that aims to meet the following desiderata

End-to-end Encryption:

In a cloud computing paradigm, we tend to assume the physical servers of cloud-based systems to be semi-trusted comparing to centralized servers behind the firewall, in that they are subjected to more malicious inside, or outside attacks, than the later one. As a result, our approach is designed to secure PHR records from the point of origin (PHR data owner) all the way to the recipient (PHR data user) in an encrypted format.

Patient-Centric

In our system, patients should have full control of their medical records and can effectively share their health data with extensive range of users. In a cryptography sense, that means patients shall generate their own decryption keys and distribute them to their authorized users.

Collusion-Resistant

In our setting, PHR data can be accessed by multiple users, such as healthcare provider, health insurer, family member etc. Hence, we cannot neglect the possibility that these users may intentionally or unintentionally collude together to gain access to part of PHR data they do not have right to access separately. For that reason, in our design, the PHR data should remain confidential under such a circumstance.

Revocation and Delegation

A PHR system is highly dynamic. Much like a social network, patients can terminate their relation with certain PHR data user, such as a health insurer, indefinitely. In other word, patients should always retain the right to revoke access privileges and its corresponding decryption key when they fell necessary. Nevertheless, data users may have the need to grant temporally part of their access right to other parties. For example, a health insurer might only allow its accounting department to access part of customers' PHR data. As a result, we should also provide a delegation mechanism in our construction. In t research, we will focus on the design and implement of a PHR system using proper cryptographic scheme. To validate our architecture, we also evaluate the applicability and efficiency of our construction.

2. RELATED WORK

Several PHR systems have been proposed or implemented to enable access control on PHR. We classify them into two categories according to their different access control mechanisms.

Authentication-Based PHR system

Some PHR systems choose an attribute-based access control (ABAC) scheme or a role-based access control (RBAC) scheme to manage users' access right. This type of system usually places full trust on the cloud server where the PHRs reside in. A typical example of authentication-based PHR system is Indivo X platform [ASZ+10]. Indivo is an open-source open standard personally controlled health record (PCHR) system that enables patients to own and manage their health records. Indivo provides patients the ability to share their records with different physicians, hospitals and clinics while maintaining access control properties on the patients' health records. Access control decisions are made by the Indivo server according to institutional policies and patient specified policies.

Cryptography based PHR system

The existing works area unit principally connected cryptographically implemented access management for outsourced data and attribute based cryptography. To understand fine-grained access management, the standard public key cryptography (PKE) based schemes [1], [2] either incur high key management transparency, or necessitate encrypting numerous copies of a files using totally different users' keys. to enhance upon the scalability of the higher than solutions, one-to-many cryptography strategies like ABE can be used. In Goyal et. al's seminal paper on ABE [3], information is encrypted underneath a group of attributes so multiple users who possess correct keys can decode. This probably makes cryptography and key management a lot of efficient [4]. An primary assets of ABE is avoiding user collusion. Additionally, the encryption is not needed to understand the ACL. A number of works used ABE to understand fine-grained access management for outsourced data [4], [5], [1], [6]. Especially, there has been Associate in tend escalating interest in applying ABE to make safe Electronic Health Records (EHRs). Recently, Narayan et al. projected Associate in Nursing attribute-based infrastructure for EHR systems, wherever every patient's EHR files area unit encrypted using a broadcast alternative to CP-ABE [7] that enables direct revocation. However, the cipher text length grow linearly with the numeral of unrevoked users. In [8], a variation of ABE that enables allocation of access rights is projected for encrypted EHRs. Ibraimi et.al. [9] applied encryption policy ABE (CP-ABE) [10] to supervise the sharing of PHRs, and introduced the proposal of professional domains. In [11], Akinyele et al. examined the usage of ABE to come up with self-protecting EMRs, which may either to be stored on cloud servers consequently EMR can be accessed when the health supplier is offline. Then again, there range unit numerous regular impairments of the higher than lives up to expectations. To begin with, they typically expect the utilization of a solitary trusty power (TA) in the framework. This may make a heap bottleneck, as well as moreover experiences the key escrow downside since the metal can get to all the encoded documents, crevice the entryway for potential security introduction. Also, it's not sensible to delegate all credit administration undertakings to one metal, including ensuring all clients' traits or parts and creating mystery keys. Truth be told, associations typically structure their own (sub)domains and get proper powers to characterize and affirm diverse sets of ascribes joy to their (sub)domains (i.e., partition and principle). as a case, an expert cooperation might be responsible for guaranteeing therapeutic strengths, while a local wellbeing supplier might ensure the work positions of its staffs. Second, there still needs Associate in Nursing proficient and on-interest client disavowal instrument for ABE with the backing for element approach overhauls/changes, that region unit key parts of secure PHR offering. At last, the majority of the predominating works don't separate between the non-open and open areas, that have completely diverse characteristic definitions, key administration necessities and versatility issues. Our arrangement of adroitly isolating the framework into 2 sorts of areas is comparative with that in [9], yet a key refinement is in [9] a solitary metal remains expected to administer the whole talented area. As of late, Yu et al. (YWRL) connected key-approach ABE to secure outsourced information in the cloud [1], [6], wherever a solitary information holder can encipher her information and offer with numerous authorized clients, by conveying keys to them that hold quality based access benefits. They furthermore propose a strategy for the information manager to renounce a client with productivity by sanction the overhauls of influenced figure writings and client mystery keys to the cloud server. Since the key upgrade operations might be totalled about whether, their plan attains low amortized overhead. Then again, in the YWRL plan, the information manager is also a metal at a comparative time. it might be wasteful to be connected to a PHR framework with various information house holders and clients, in light of the fact that then every client might accept numerous keys from different house managers, regardless of the fact that the keys hold the same sets of qualities. On the inverse hand, Chase and Chow [12] anticipated a numerous power ABE (CC MAABE) reply inside which various Tas, each administering an unique set of the framework's clients' qualities, produce client mystery keys conjointly. A client needs to acquire one a piece of her key from each metal. This plan forestalls against plot around at most N − a couple of Tas, moreover to client conspiracy safety. On the other hand, its not clear an approach to acknowledge effective client denial. Moreover, since CC MA-ABE installs the right to gain entrance strategy in clients' keys as opposed to the figure message, a prompt provision of it to a PHR framework is non-instinctive, as it is not clear an approach to permit information house holders to point out their document access arrangements. Disavowal is carried out chiefly manual Associate in Nursing access table is kept up for client PHR record and client information is kept in this right to gain entrance table. When renouncement is carried out the client information is off from the right to gain entrance table. This response is not versatile in light of the fact that the PHR client increases. We require a versatile respond in due order regarding this downside.

3. OVERVIEW OF OUR APPROACH

Personal Health Record is an internet based application that allows people to access and co-ordinate their lifelong health information and make if appropriate parts of its available to those who need. Personal Health Record's security and protection of its data have immense apprehension and area of research over the years. Several cryptographic mechanisms like AES, MD5 proposed to guarantee data security. In this paper we propose an inimitable encryption as well as authentication technique using AES algorithm. The proposed system architecture is shown in Fig.1

3.1 Attribute Hierarchy

We use attribute based encryption for providing security. For that we use following attribute distribution process within PHR as shown in Fig.2

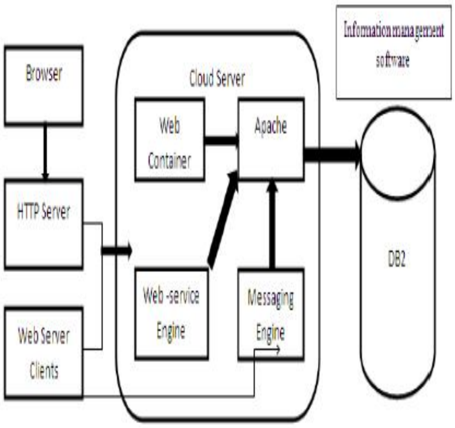

Figure 1 PHR Architecture

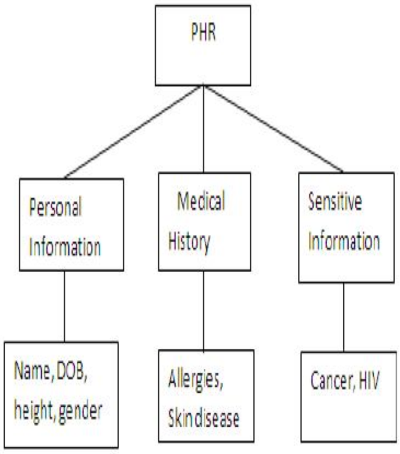

Figure 2 PHR Attributes

3.2 Advanced Encryption Standard

AES is an Advanced Encryption Standard used for secure transmission of data that is personal health record in encrypted format. In our system AES is used for sending user authentication data in encrypted format. AES allows three diversed key lengths: 128, 192, or 256 bits.

For encryption, each round consist of the following four step

- Substitute bytes
- Shift rows
- Mix columns
- Add round key

The last step consists of XORing the output of the previous three steps. For decryption, every round includes the following four steps

1. Inverse shift rows
2. Inverse substitute bytes
3. Add round key
4. Inverse mix columns.

The third step consists of XORing the output of the previous two steps

Step1: Substitute bytes

- This step consists of using a 16 × 16 research table to find out a replacement byte for a given byte within the input state array.
- The entries in the table are created by using the philosophy of summative inverses in GF (28) as well as scrambled bit to destroy the bit-level correlations inside every byte.

Step2: Shift rows

- The primary row of state is not altered.
- The second row is shifted 1 byte to the left in a circular manner.
- The third row is shifted 2 bytes to the left in a circular manner.
- The fourth row is shifted 3 bytes to the left in a circular manner.

Step3: Mix columns

- Mix Columns for integration up of the bytes in every column individually during the process.
- This step replaces each byte of a column by a function of all the bytes in the same column.

Step4: Add round key

- Add Round Key to add the round key to the output of the cumulative step during the forward process
- In this stage, the 128 bits are bitwise XORed along with the 128 bits of the round key.
- The operation is viewed as column wise operation between is 4 bytes of status column along with one word of the round key.

4. CONCLUSION

Our Proposed System Quickly find out information of patient details. In case of emergency the doctor and other emergency department can quickly get all the details of all the informative details and start treatment. If in any condition doctors and medical facilities are not available the PHR owner itself able to take care of his health. This paper proposed the new approach for existing PHR system for providing more security using attribute based encryption which plays an important role because these are unique and not easily hackable. We are reducing key management problem and also we enhance privacy guarantee.

References

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

[2] 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.

[3] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEEWireless Communications Magazine, Feb. 2010.

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

[5] 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.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010. [30] S. Kurosawa, H. Nakayama, N. Kato, and A. Jamalipour,

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

[8] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in AHIC 2010, 2010.

[9] L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," Technical Report, University of Twente, 2009.

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

[11] 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, 2010, http://eprint.iacr.org/.

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