International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 8, ISSN No. 2455-2143, Pages 61-65
Published Online December 2018 in IJEAST (http://www.ijeast.com)

USING MULTI -ATTRIBUTE BASED ENCRYPTION SECURE SHARING OF PERSONAL HEALTH RECORD IN CLOUD

Shruthi N
Asst. Prof, Department of ISE
MVJCE, Bangalore, Karnataka, INDIA

***Abstract*— Personal health record (PHR) is a patient-centric model for health information exchange which is stored at third party, such as cloud providers which is a semi-trusted servers. There have been a wide privacy concerns that personal health information could be exposed to unauthorized parties. To assure patients' control over access to their own PHRs before outsourcing issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges towards achieving fine-grained, cryptographically enforced data access control. For fine-grained and scalable data access control for PHRs, there is a leverage of attribute based encryption (ABE) techniques to encrypt each patient PHR file. Different from previous work on secure data outsourcing, here it is focused on multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces key management complexity for owners and users.**

Keywords— **Attribute-based encryption, cloud computing, data privacy, Personal health records**

I. INTRODUCTION

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. It had never been easier than now for one to create and manage their own personal health information (PHI) in one place, and share that information with others. It enables a patient to merge potentially separate health records from multiple geographically dispersed health providers into one centralized profile over passages of time. This greatly facilitates multiple other users, such as medical practitioners and researchers to gain access to and utilize one's PHR on demand according to their professional need, thereby making the healthcare processes much more efficient and accurate. Due to the high cost of building and maintaining specialized data centres, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft Health Vault. Recently, architectures of storing PHRs in cloud computing have been proposed in L¨ohr H Et. al(2010)[2], Li M Et. al(2011)[3].

Despite enthusiasm around the idea of the patient-centric PHR systems, their promises cannot be fulfilled until we address the serious security and privacy concerns patients have about these systems, which are the main impediments standing in the way of their wide adoption. In fact, people remain dubious about the levels of privacy protection of their health data when they are stored in a server owned by a third-party cloud service provider. Most people do not fully entrust the third-party service providers for their sensitive PHR data because there is no governance about how this information can be used by them and whether the patients actually control their information. For example, although there exist healthcare regulations for EMRs, such as HIPAA which is recently amended to incorporate business associates in 2009 [4], several cloud providers are not covered entities by them (2009)[5].

Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary Mandl K. D Et. al(2001)[7]. The authorized users may either need to access the PHR for personal use or professional purposes. Examples of the former are family member and friends, while the latter can be medical doctors, pharmacists, and researchers, etc.

Here it's referred to the two categories of users as personal and professional users, respectively. The latter has potentially large scale; should each owner oneself be directly responsible for managing all the professional users, they will easily be overwhelmed by the key management overhead. On the other hand, different from the single data owner scenario considered in most of the existing works Benaloh J Et. al (2009)[8], Yu S Et. al(2010) [9], in a PHR system, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. In order to protect the personal health data stored on a semi-trusted server, here its

International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 8, ISSN No. 2455-2143, Pages 61-65
Published Online December 2018 in IJEAST (http://www.ijeast.com)

adopted 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 their 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.

II. FRAMEWORK FOR PATIENT-CENTRIC, SECURE AND SCALABLE PHR SHARING

In this section, it is described about novel patient-centric secure data sharing framework for cloud-based PHR systems.

A. Problem Definition

This paper is mostly related to works in cryptographically 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 management 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 encryption methods such as ABE can be used. In Goyal Et. al seminal paper on ABE, data is encrypted under a set of attributes so that multiple users who possess proper keys can decrypt. This potentially makes encryption and key management more efficient.

B. Security model

In this model, it's been considered the server to be semi-trusted, i.e., honest but curious as those in Yu S Et. al(2010)[15]. That means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collude with other users, or even with the server. In addition, it's assumed each party in this system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols.

C. Requirements

To achieve "patient-centric" PHR sharing, a core requirement is that each patient can control who are authorized to access to their own PHR documents. Especially, user controlled read/write access and revocation are the two core security objectives for any electronic health record system, pointed out by Mandl Et. al [7] in as early as 2001. The security and performance requirements are summarized as follows:

• Data confidentiality: Unauthorized users (including the server) who do not possess enough attributes satisfying the access policy or do not have proper key access privileges should be prevented from decrypting a PHR document, even under user collusion. Fine-grained access control should be enforced, meaning different users are authorized to read different sets of documents.

• On-demand revocation: Whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute. This is usually called attribute revocation, and the corresponding security property is forward secrecy Hur J Et. al(2010)[23]. There is also user revocation, where all of a user's access privileges are revoked.

• Write access control: Its prevented unauthorized contributors to gain write-access to owners' PHRs, while the legitimate contributors should access the server with accountability.

• The data access policies should be flexible, i.e., dynamic changes to the predefined policies shall be allowed, especially the PHRs should be accessible under emergency scenarios.

D. Overview of Framework

The main goal of this framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains (PUDs) and personal domains (PSDs)) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner.

In both types of security domains, we utilize ABE to realize cryptographically enforced, patient-centric PHR access. Especially, in a PUD multi-authority ABE is

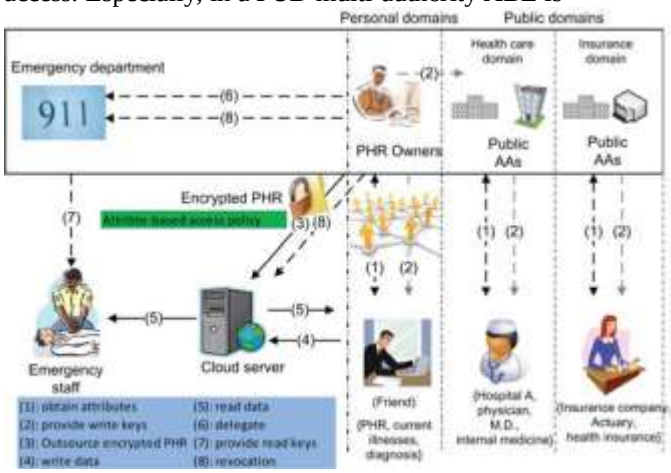

Fig 1: The proposed framework for patient-centric, secure and scalable PHR sharing on semi-trusted storage under multi-owner settings.

used, in which there are multiple "attribute authorities" (AAs), each governing a disjoint subset of attributes. *Role attributes*

International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 8, ISSN No. 2455-2143, Pages 61-65
Published Online December 2018 in IJEAST (http://www.ijeast.com)

are defined for PUDs, representing the professional role or obligations of a PUD user. Users in PUDs obtain their attribute-based secret keys from the AAs, without directly interacting with the owners. To control access from PUD users, owners are free to specify role-based fine-grained access policies for her PHR files, while do not need to know the list of authorized users when doing encryption. Since the PUDs contain the majority of users, it greatly reduces the key management overhead for both the owners and users.

Each data owner (e.g., patient) is a trusted authority of their own PSD, who uses a KP-ABE system to manage the secret keys and access rights of users in their PSD. Since the users are personally known by the PHR owner, to realize patient-centric access, the owner is at the best position to grant user access privileges on a case-by-case basis. For PSD, *data attributes* are defined which refer to the intrinsic properties of the PHR data, such as the category of a PHR file. For the purpose of PSD access, each PHR file is labelled with its data attributes, while the key size is only linear with the number of file categories a user can access. Since the number of users in a PSD is often small, it reduces the burden for the owner. When encrypting the data for PSD, all that the owner needs to know is the intrinsic data properties.

The multi-domain approach best models different user types and access requirements in a PHR system. The use of ABE makes the encrypted PHRs self-protective, i.e., they can be accessed by only authorized users even when storing on a semi-trusted server, and when the owner is not online. In addition, efficient and on-demand user revocation is made possible via our ABE enhancements.

III. MODULE DESCRIPTION

A. Admin support system

In this module used to control all the process. Administration is a dynamic work in every field. The initial meaning of administration is the running of a business or system. In every step of your business, it needs administration. To run faster in the technological scenario a business need to administer.

In our project administrative support service in various administrative levels rightly starts from:

- Admin management
- Hospital management
- Pharmacy management

Fig 2:Admin support system

A. Data Privacy System [MA-ABE]

In this multi-authority ABE module, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users and encryptions can require that a user obtain keys for appropriate attributes from each authority before decrypting a message.

Attribute-Based Encryption (ABE) scheme that allows a user's private key to be expressed in terms of any access formula over attributes. Previous ABE schemes were limited to expressing only monotonic access structures. It is provide a proof of security for our scheme based on the data privacy system.

Fig 3: Data privacy system

B. Patient Care System

In this Patient Care System is a computer-based "patient record system" which facilitates an electronic patient encounter, helping automate the entire clinical workflow. This allows capture of medical data in a standard format, making its collection, comparison and use across the health care spectrum quick and efficient. In our Healthcare organizations require comprehensive information management to ensure that vital patient information is always available to caregivers at point-of-care. A well-designed patient care system can streamline workflow, reduce the risk of medical errors and improve the patient care experience for caregivers and patients alike.

The patient care framework establishes and generates the clinical tools needed to manage the delivery of patient care. Combined with hospital management solution, the patient care framework covers functional areas such as diagnosis, review details, inpatient & outpatient management, doctors' appointment diary, prescriptions, operation theatre management and the like. The system provides for extensive MIS reports and the data can be used for research and analysis.

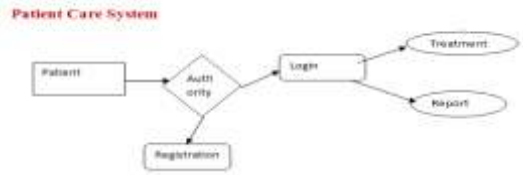

Fig 4: Patient care system

C. Data Provider System

In this module provider is an individual or an institution that provides preventive, curative, promotional or rehabilitative health care services in a systematic way to individuals, families or communities. This data service provider maintains large amount of patient database and maintains all record in order to transfer and deliver content to

International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 8, ISSN No. 2455-2143, Pages 61-65
Published Online December 2018 in IJEAST (http://www.ijeast.com)

those paying the subscription fee. A data service provider that comprehensively handles the client needs of their client from concept to installation through support. This process normally involves studying the client's current infrastructure, evaluating the client's needs, specifying the mix of manufacturers' records and details required to meet client goals at the client's site(s).

Computer-based patient record (CPR) systems form the infrastructure for the timely and accurate collection and exchange of data, information, and knowledge in healthcare organizations, and thus a more efficient use of scarce resources.

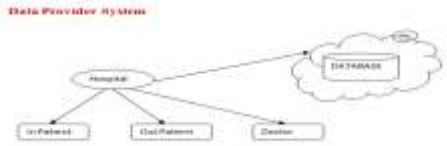

Fig 5: Data provider system

D. Health Information Exchange

In this Health Information Exchange (HIE) refers to the process of reliable and interoperable electronic health-related information sharing conducted in a manner that protects the confidentiality, privacy, and security of the information. The development of widespread HIEs is quickly becoming a reality.

i) Personal Report

Personal data is information that relates to living individuals. It does not include information relating to the deceased or to groups or communities of people information.

Personal information is about the patient details. It is including names, addresses and dates of birth, as well as information relating to the services which individuals receive from the Council.

ii) Professional Report

The professional report is a claim by the Department of Health that patient data shared with private firms for medical research would be anonymised has been challenged by privacy campaigners. It is used to further research and another treatment. All the research people access the patient professional reports. It is only for doctors and also research peoples.

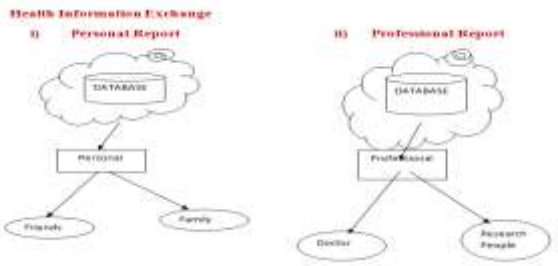

Fig 6: Health information exchange

IV. TECHNIQUE USED: MULTI-AUTHORITY ABE (MA-ABE)

Multi-authority ABE (MA-ABE) is to improve the security and avoid key escrow problem. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system. Here its proposed mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes. Furthermore, we enhance MA-ABE by putting forward an efficient and on-demand user/attribute revocation scheme, and prove its security under standard security assumptions. In this way, patients have full privacy control over their PHRs.

V. APPLICATIONS

B. Child patient care

Boston Children's Hospital is a 395-bed comprehensive centre for pediatric health care. As one of the largest pediatric medical centres in the United States, Children's offers a complete range of health care services for children from birth through 21 years of age. (Our Advanced Fetal Care Center can begin interventions at 15 weeks gestation, and in some situations, we treat adults.)

Children's records approximately 24,943 inpatient admissions each year, and our 228 specialized clinical programs schedule more than 557,620 visits annually. Additionally, the hospital performed 26,534 surgical procedures and 158,791 radiological examinations last year.

B. Research

Children's is home to the world's largest research enterprise based at a pediatric hospital. More than 1,100 scientists, including nine members of the National Academy of Sciences, 11 on-staff members of the Institute of Medicine and 9 members of the Howard Hughes Medical Institute, comprise our research community. Current initiatives have attracted a record $225 million in annual funding, including more federal funding than any other pediatric facility.

C.INDIVO Health

Indivo is the original personal health platform, enabling an individual to own and manage a complete, secure, digital copy of her health and wellness information. Indivo integrates health information across sites of care and over time. Indivo is free and open-source uses open, unencumbered standards, including those from the SMART Platforms project and is actively deployed in diverse settings.

International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 3, Issue 8, ISSN No. 2455-2143, Pages 61-65
Published Online December 2018 in IJEAST (http://www.ijeast.com)

VI. CONCLUSION

Proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, it's argued that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that it's greatly reduced the complexity of key management while enhance the privacy guarantees compared with previous works. Here it is utilized ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations. Furthermore, also enhanced an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, it is shown that the given solution is both scalable and efficient.

VII. REFERENCE

[1] Li M, Yu S, Ren K, and Lou W, (Sept. 2010) "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings", in *SecureComm'10*, (pp. 89–106).

[2] L¨ohr H, Sadeghi A R., and Winandy M., (2010)"Securing the e-health cloud," in *Proceedings of the 1st ACM International Health Informatics Symposium*, ser. IHI '10, (pp. 220–229).

[3] Li M, Yu S, Cao N, and Lou W,(JUNE,2011) "Authorized private keyword search over encrypted personal health records in cloud computing," in *ICDCS* .

[4] "The health insurance portability and accountability act." [Online].Available: http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp

[5] "Google, microsoft say hipaa stimulus rule doesn't apply to them," http://www.ihealthbeat.org/Articles/2009/4/8/.

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

[7] Mandl K. D, Szolovits P, and Kohane I. S, (Feb. 2001)"Public standards and patients' control: how to keep electronic medical records accessible but private," *BMJ*, (vol. 322, no. 7281, p. 283).

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

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

[10] Dong C, Russello G, and Dulay N, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security.

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

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

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

[14] Ibraimi L, Petkovic M, Nikova S, Hartel P, and Jonker W, (2009)"Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes".

[15] Yu S, Wang C, Ren K, and Lou W,(2010), "Attribute based data sharing with attribute revocation," in ASIACCS'10.

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

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

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

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

[20] Akinyele J. A, Lehmann C. U, Green M. D, Pagano M. W, Peterson Z. N. J, and Rubin A. D,(2010), "Self-protecting electronic medical records using attribute-based encryption," Cryptology ePrint Archive, Report 2010/565, http://eprint.iacr.org/.

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

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

[23] Hur J and Noh D. K,(2010), "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, (vol. 99).

[24] Jahid S, Mittal P, and Borisov N,(March,2011), "Easier: Encryption-based access control in social networks with efficient revocation," in ASIACCS, Hong Kong.