International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 23rd Apr 2019. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-04

Title: A SURVEY ON SECURITY PERSONAL HEALTH RECORDS IN CLOUD COMPUTING

Volume 08, Issue 04, Pages: 324–331.

Paper Authors

ADIMULAM RAGHU BABU, M.TILAK

SKBR PG College, Amalapuram

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A SURVEY ON SECURITY PERSONAL HEALTH RECORDS IN CLOUD COMPUTING

[1]ADIMULAM RAGHU BABU, [2]M.TILAK
[1]PG Scholar, Department of MCA, SKBR PG College, Amalapuram
[2]Assistant Professor, Department of MCA, SKBR PG College, Amalapuram

Abstract -- The Personal Health Record (PHR) is an emerging framework of health information exchange, which is often stored at cloud servers. But there are still various privacy problems as personal health information could be discovered to unauthorized people. To guarantee the patients control over to their own PHRs, it is a method to encrypt the PHRs before storing on cloud. But still issues such as risks of privacy, efficiency in key administration, flexible access and efficient user administration, have still remained the important challenges toward achieving better, cryptographically imposed data access control. Here in this research paper, we develop a model and mechanism for control of data access to PHRs stored in cloud servers. To achieve efficient and modular data access control for PHRs, we provide ABE encryption approach to encrypt each PHR file. In this system we try to focus on the multiple data owner scheme, and divide the users into security domains that highly reduce the key management complication for owners and users. In this system patient privacy is guaranteed by exploiting multi-authority ABE. Our system's scheme also enables modification of access policies or file attributes, and break-glass access under emergency situations. Extensive analysis and experimental results are presented which shows the security and efficiency of our proposed scheme.

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

I.INTRODUCTION

Cloud computing has emerged as an important computing paradigm to offer pervasive and ondemand availability of Various resources in the form of hardware, software, infrastructure, and storage [1, 2]. Consequently, the cloud computing paradigm facilitates organizations by relieving them from the protracted job of infrastructure development and has encouraged them to trust on the third-party Information Technology (IT) services [3]. Additionally, the cloud computing model has demonstrated significant potential to increase coordination among several healthcare stakeholders and also to ensure continuous availability of health information, and scalability [4, 5]. Furthermore, the cloud computing also integrates various important entities of healthcare domains, such as patients, hospital staff including the doctors, nursing staff, pharmacies, and clinical laboratory personnel, insurance providers, and the service providers [6].

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Therefore, the integration of aforementioned entities results in the evolution of a cost effective and collaborative health ecosystem where the patients can easily create and manage their Personal Health Records (PHRs) [7]. Generally, the PHRs contain information, such as: (a) demographic information, (b) patients' medical history including the diagnosis, allergies, past surgeries, and treatments, (c) laboratory reports, (d) data about health insurance claims, and (e) private notes of the patients about certain important observed health conditions [8]. More formally, the PHRs are managed through the Internet based tools to permit patients to create and manage their health information as lifelong records that can be made available to those who need the access [9]. Consequently, the PHRs enable the patients to effectively communicate with the doctors and other care providers to inform about the symptoms, seek advice, and keep the health records updated for accurate diagnosis and treatment. Despite the advantages of scalable, agile, cost effective, and ubiquitous services offered by the cloud, various concerns correlated to the privacy of health data also arise. A major reason for patients' apprehensions regarding the confidentiality of PHRs is the nature of the cloud to share and store the PHRs [10]. Storing the private health information to cloud servers managed by thirdparties is susceptible to unauthorized access. In particular, privacy of the PHRs stored in public clouds that are managed by commercial service providers is extremely at risk [11]. The privacy of the PHRs can be at risk in several ways, for example theft, loss, and leakage [12]. The PHRs either in cloud storage or in transit from the patient to the cloud or from cloud to any other user may be susceptible to unauthorized access because of the malicious behavior of external entities. Moreover, there are also some threats by valid insiders to the data [13]. For instance, the PHRs either in cloud storage or in transit from the patient to the cloud or from cloud to any other user may be susceptible to unauthorized access because of the malicious behavior of external entities [10]. The individuals working at the cloud service provider can behave maliciously. A popular example for that is an incident when an employee of the Department of Veterans Affairs of the U.S. carried homethe sensitive personal health information of around 26.5 million without any authorization [14].

II. RELATED WORK

This paper is based on the works in cryptograph-icily enforced access control for the data stored in cloud and attribute based encryption. To apply fine-grained access control, the conventional public key encryption (PKE) based techniques either include high key management overhead, or require encrypting copies of a file using different set of users keys. To enhance the scalability of the solutions mentioned above, encryption schemes like ABE can be used. Here in Goya paper on ABE information is encrypted under a group of attributes so that multiple users who have proper keys can decrypt it. Thus it makes encryption and key management more efficient. Fine-grained Data Access Control using ABE: The

numerous schemes use ABE to understand fine-grained access control for outsourced data. Specially, there has been an increase in interest in applying ABE based encryption schemes to protect electronic healthcare records (EHRs).Lately, Narayan recommended an attribute-based framework for an electronic healthcare records systems, where each users(patient) EHR files are encrypted using a variant of CPABE that allows direct revocation. But however, the cipher text range grows sequentially with the numerous of unrevoked users. Here in another scheme of ABE that allows relegation of access rights is used for encrypted EHRs. Ibraimi applied cipher text policy ABE to maintain the sharing of PHRs, and popularized the theory of social/professional domains. Here in, Akinyele investigated using ABE to generate self-assured EMRs, which can each of two can be stored on cloud servers or mobile devices so that EMR could be gained when the health provider is offline. But however, there are various familiar drawbacks of the above works. Here, they will usually consider the use of a one separate trusted authority (TA) in the structure. It may create a load bottleneck, and it also may undergo the key escrow issue since the TA can acquire all the encrypted files, which may lead to privacy disclosure. Also in addition, it is not practically acceptable to give all attribute administrative functions to one TA, along with certifying all users‟ attributes or roles and generating secret keys. Different organizations usually form their own domains and become authorities to define and approve different sets of attributes belonging to their concern (i.e., divide and rule). Let's say for e.g., an experienced professional association would be responsible for certifying professional medical specialties, elsewhere a regional health provider would authorize the job ranks of its staffs. But, there still lacks an efficient and on-call user revocation structure for ABE with the backing for productive policy updates, which are crucial elements of secure PHR sharing.

In PHR system data is outsourced on data server over internet. For privacy and security of information, encryption techniques are. Cryptography is used to provide privileges. For smoother access privileges, the traditional public key encryption (PKE) may costs excess key management overhead and scalability issue. For more scalable PKE, ABE can be used. In Goyal et al.s seminar papers on ABE [14], data encryption is done using set of attributes so that multiple users that have proper keys can decrypt. Attribute-based encryption (ABE) is a new technique that uses the concept of public-key cryptography. ABE defines the identity as set of attributes not limited to single atomic key as in PKE. There are different versions of ABE as MAABE (Multi-authority ABE), CP-ABE (Cipher-text Policy ABE) and KP-ABE (key-policy ABE). The traditional public key encryption (PKE) can be used to achieve fine-grained access. KP-ABE algorithm used for access control in PHRs. But KP-ABE lacks the efficiency and security of the scheme. Because of the data owner is also the TA (rusted Authority) and

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

the program didn't changes the random parameter of ABE it has efficiency problem. To solve the efficiency problem of KP-ABE, a MA-ABE access control strategy is used. 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.

III. PROPOSED SYSTEM

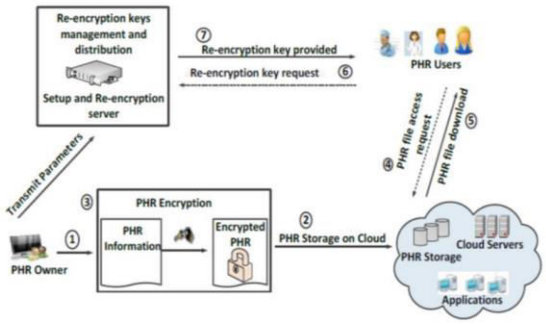

Fig. 1: PROPOSED SYSTEM

The proposed scheme employs proxy re-encryption for providing confidentiality and secure sharing of PHRs through the public cloud. The architecture of the proposed SeSPHR methodology is presented in Fig. 1. Entities The proposed methodology to share the PHRs in the cloud environment involves three entities namely:

(a) the cloud,

(b) Setup and Re-encryption Server (SRS), and

(c) the users. Brief description about each of the entities is presented below.

The Cloud: The scheme proposes the storage of the PHRs on the cloud by the PHR owners for subsequent sharing with other users in a secure manner. The cloud is assumed as un-trusted entity and the users upload or download PHRs to or from the cloud servers. As in the proposed methodology the cloud resources are utilized only to upload and download the PHRs by both types of users, therefore, no changes pertaining to the cloud are essential. Setup and Re-encryption Server (SRS): The SRS is a semi-trusted server that is responsible for setting up public/private key pairs for the users in the system. The SRS also generates the re-encryption keys for the purpose of secure PHR sharing among different user groups. The SRS in the proposed methodology is considered as semitrusted entity. Therefore, we assume it to be honest following the protocol generally but curious in nature. The keys are maintained by the SRS but the PHR data is never transmitted to the SRS. Encryption and decryption operations are performed at the users' ends. Besides the key management, the SRS also implements the access control on the shared data. The SRS is independent server that cannot be deployed over a public cloud because of cloud being untrusted entity. The SRS can be maintained by a trusted third-party organization or by a group of hospitals for convenience of the patients. It can also be maintained by a group of connected patients. However, SRS maintained by hospitals or by a group of patients will generate more trust due to involvement of

health professionals and/or self-control over SRS by patients. Users: Generally, the system has two types of users: (a) the patients (owners of the PHR who want to securely share the PHRs with others) and (b) the family members or friends of patients, doctors and physicians, health insurance companies' representatives, pharmacists, and researchers. In SeSPHR methodology, the friends or family members are considered as private domain users whereas all the other users are regarded as the public domain users. The users of both the private and public domain may be granted various levels of access to the PHRs by the PHR owners. For example, the users that belong to private domain may be given full access to the PHR, whereas the public domain users, such as physicians, researchers, and pharmacists may be granted access to some specific portions of the PHR. Moreover, the aforementioned users may be allowed full access to the PHRs if deemed essential by the PHR owner. In other words, the SeSPHR methodology allows the patients to exercise the fine-grained access control over the PHRs. All of the users in the system are required to be registered with the SRS to receive the services of the SRS. The registration is based on the roles of the users, for instance, doctor, researcher, and pharmacist.

The PHR is logically partitioned into the following four portions:

• Personal Information;
• Medical information;
• Insurance related information;
• Prescription information;

However, it is noteworthy that the above said partitioning is not inflexible. It is at the discretion of the user to partition the PHR into lesser or more number of partitions. The PHRs can be conveniently partitioned and can be represented in formats, for example XML. Moreover, the PHR owner may place more than one partition into same level of access control. Any particular user might not be granted a full access on the health records and some of the PHR partitions may be restricted to the user. For example, a pharmacist may be given access to prescription and insurance related information whereas personal and medical information may be restricted for a pharmacist. Likewise, family/friend may be given full access to the PHR. A researcher might only need the access to the medical records while de-identifying the personal details of the patients. The access rights over different PHR partitions are determined by the PHR owner and are delivered to the SRS at the time of data uploading to the cloud.The proposed methodology provides the following services for the PHRs shared over the public cloud.

• Confidentiality;
• Secure PHR sharing among the groups of authorized users;
• Securing PHRs from unauthorized access of valid insiders;
• Backward and forward access control; In the proposed methodology, the cloud is not considered a trusted entity. The features of cloud computing paradigm, such as shared pool of resources, multi tenancy, and virtualization might generate many sorts of insid-er and outsider threats to the PHRs that

are shared over the cloud. Therefore, it is important that the PHRs should be encrypted before storing at the third-party cloud server. The PHR is first encrypted at the PHR owner's end and is subsequently uploaded to the cloud. The cloud merely acts as a storage service in the proposed methodology. The encryption keys and other control data are never stored on the cloud. Therefore, at the cloud's end the confidentiality of the data is well achieved. Even if the unauthorized user at the cloud by some means obtains the encrypted PHR file, the file cannot be decrypted because the control data does not reside at the cloud and the confidentiality of the PHR is ensured. The uploaded PHRs are encrypted by the owner and the rest of the users obtain the plain data by utilizing the re-encryption key that is computed by the SRS. The SRS generates the re-encryption parameters only for the allowed partitions corresponding to the requesting user. Therefore, the privacy of the entire system is not disturbed by a compromised legitimate group member. The ACL specifies all the rights pertaining to each of the users and are specified by the PHR owner. The rights are specified based on the categories of the users and are extended/limited by the approval of the PHR owner. The SRS calculates and sends the re-encryption parameters based on the specified rights on the partitions. Therefore, even the legitimate users cannot access the unauthorized partition. The newly joining member obtains the keys from the SRS. The shared data is encrypted by the keys of the owner only. The access to the data for newly joining member is granted by the approval of the SRS. Moreover, introducing a new key in the system does not require reencryption of the whole data. Similarly, a departing user is removed from the ACL and the corresponding keys are deleted. The deletion of the user keys and removal from the ACL results in denial of access to the PHR for any illegitimate access attempts afterwards. Therefore, the proposed methodology is effectively secure because it restricts the access of departing users (forward access control) and permits the new users to access the past data (backward access control). The SRS is considered a semi-trusted authority that is honest but curious. In general, the SRS is assumed to follow the protocol honestly. Although the SRS generates and stores the key pair for each of the users, the data whether encrypted or plain is never transmitted to the SRS. The SRS is only responsible for key management and re-encryption parameters generation. Moreover, the access control is also enforced by the SRS. However, maintenance of the SRS is the limitation and challenge of the proposed methodology.

IV. RESULTS

Figures shows storage cost, execution time and performance analysis of encryption algorithms. As compare to other encryption algorithm, ABE and Blowfish has equal storage cost, lowest execution cost and highest performance. So ABE and Blowfish is best option for providing security in PHR system.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

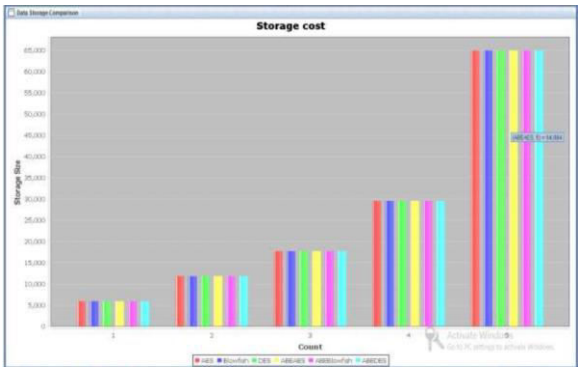

Fig. 2: COMPARISON OF STORAGE COST

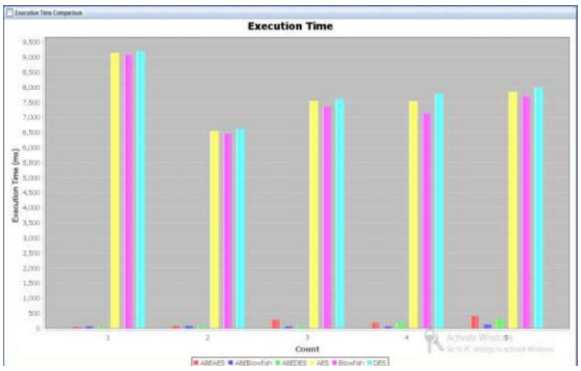

Fig. 3: COMPARISON OF EXECUTION TIME

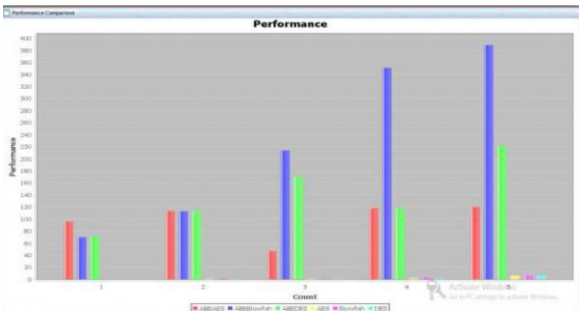

Fig. 4: OVERALL PERFORMANCE

V. CONCLUSION

There was widespread consensus at the College's symposium about the potential value of PHR systems. Participants elucidated the potential of PHR systems to transform patient–provider relationships, especially when integrated with EHR systems. They also identified many challenges—technical, social, organizational, legal, and financial—that warrant further study. PHRM systems plus points are described by users that transform patient provider relationships. Especially when it is integrated with EHR systems. PHRM has many that must be considered for further study like technical, social, organizational, legal, and financial. Users and organizations related to medical field fast adopt PHRMs. Many challenges to deployment of PHRMs are similar to those for EHRs. More PHRM-related research is required. In PHRM every entity such as employers, patients, payers, governments, and research institutions must play key roles in developing PHRM to overcome the problems to widespread adoption. With a better understanding of the needs and benefits of PHRMs, we can develop better solution. The opportunity costs for PHR deployment are measured in medical errors, dollars, and lives. If the potential benefits are to realize for both routine health care and for responding to catastrophic disasters like Hurricane Katrina, these important PHR-related issues must be addressed.

VI. REFERENCE

[1] K. Gai, M. Qiu, Z. Xiong, and M. Liu, "Privacy-preserving multi-channel communication in Edge-of-Things," Future Generation Computer Systems, 85, 2018, pp. 190-200.

[2] K. Gai, M. Qiu, and X. Sun, "A survey on FinTech," Journal of Network and Computer Applications, 2017, pp. 1-12.

[3] A. Abbas, K. Bilal, L. Zhang, and S. U. Khan, "A cloud based health insurance plan recommendation system: A user centered approach, "Future Generation Computer Systems, vols. 43- 44, pp. 99-109, 2015.

[4] A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Shamshirband, "Incremental proxy re-encryption scheme for mobile cloud computing environment," The Journal of Supercomputing, Vol. 68, No. 2, 2014, pp. 624-651.

[5] R. Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," In 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Work-

[6] A. Abbas and S. U. Khan, "A Review on the State-of-the-Art Privacy Preserving Approaches in E-Health Clouds," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 4, pp. 1431-1441, 2014.

[7] M. H. Au, T. H. Yuen, J. K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L. Jiang, "A general framework for secure sharing of personal health records in cloud system," Journal of Computer and System Sciences, vol. 90, pp, 46-62, 2017. [8] J. Li, "Electronic personal health records and the question of privacy," Computers, 2013, DOI: 10.1109/MC.2013.225.

[9] D. C. Kaelber, A. K. Jha, D. Johnston, B. Middleton, and D. W. Bates, "A research agenda for personal health records (PHRs)," Journal of the American Medical Informatics Association, vol. 15, no. 6, 2008, pp. 729-736.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in Proceedings of the IEEE INFOCOM, March 2010, pp. 1-9.

[11] S. Kamara and K. Lauter, "Cryptographic cloud storage," Financial Cryptography and Data Security, vol. 6054, pp. 136–149, 2010.

[12] T. S. Chen, C. H. Liu, T. L. Chen, C. S. Chen, J. G. Bau, and T.C. Lin, "Secure Dynamic access control scheme of PHR in cloud computing," Journal of Medical Systems, vol. 36, no. 6, pp. 4005– 4020, 2012.

[13] K. Gai, M. Qiu, "Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers," IEEE Transactions on Industrial Informatics, 2017, DOI: 10.1109/TII.2017.2780885.

[14] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, 2013, vol. 24, no. 1, pp. 131–143.

[15] "Health Insurance Portability and Accountability,"http://www.hhs.gov/ocr/privacy/hipaa/administrative/pr ivacyrule/, accessed on October 20, 2014.