International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

Secure Sharing Of PHR Data Using Reencryption

CHINDRIPU. JEMERIS CHERIAN #1, S.CHITTIBABULU #2
1Student, Computer Science and Engineering, NOVA College of Engineering and Technology, Vegavaram(V), Jangareddigudem(M) West Godavari(D) Andhra Pradesh
2Guide, Associate Professor, Computer Science and Engineering, NOVA College of Engineering and Technology, Vegavaram(V), Jangareddigudem(M) West Godavari(D) Andhra Pradesh

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. ABE. This paper we proposes a methodology called SeSPHR for secure sharing of the PHRs in the cloud. The SeSPHR scheme ensures patient-centric control on the PHRs and preserves the confidentiality of the PHRs. The patients store the encrypted PHRs on the un-trusted cloud servers and selectively grant access to different types of users on different portions of the PHRs. A semi-trusted proxy called Setup and Re-encryption Server (SRS) is introduced to set up the public/private key pairs and to produce the re-encryption keys. Moreover, the methodology is secure against insider threats and also enforces a forward and backward access control. Furthermore, we formally analyze and verify the working of SeSPHR methodology through the High Level Petri Nets (HLPN).

I. Introduction

A PHR is information about the health of a patient, compiled and maintained by the patient himself. This can be used to track and share an individual's past and current health information. PHR is also a tool for global medical data sharing. Thus an authorized medical care provider can have access to a patient's health related information and thereby gains more insight into the health history of the patient under his care. To overcome the obstacles arising as a result of scalability problems, many PHR services are outsourced to third party servers like the clouds.

Cloud Computing, one of the most powerful paradigms in the IT sector, is a way to increase capacity on the fly without investing in new infrastructure, training new personnel, or licensing new software. However cloud computing means storage of data on the internet. The outsourcing of PHR data on to clouds has led to concerns of the insecurity of the medical information. The medical information of an individual is highly sensitive and must be accessed

only by the patient or by those who has been given authorization by the patient. The data must remain confidential to all else.

A solution to this dilemma is to encrypt the information before uploading for storage in clouds. There has been various techniques proposed for the encryption of data outsourced to clouds. One method is the usage of passwords provided by the owner/patient whenever access to a PHR file is needed. Another mechanism is the presence of a Central Trusted Authority. But all these techniques have limitations. The usage of passwords requires a PHR owner/patient to be continuously online, which is not feasible. Central Authority can lead to a single point of failure. A better suggestion, which has also been effectively implemented, is the Attribute Based Encryption (ABE) scheme. Users of the PHR service are given access to a PHR file only if they have been authorized by the PHR owner/patient, i.e., the patient. A patient's PHR file can be accessed by his relatives, friends, doctors, nurses etc. If the owner/patient is responsible for managing all details of each user key, then, keeping in mind the large and unlimited number of possible professional users, there could be heavy key management overhead.

To solve the key management issues and also taking into account the multi-owner/patient scenario, Ming Li proposed a scheme, in [1], where, a patient PHR user profile can be divided into two categories or domains, one being the private domain, which consists of his friends and relatives, and the other being the public domain, which consists of the medical professionals who are authorized to view his medical files, and, managing both domains by different means. He propounded the usage of Multi-Authority ABE (MA-ABE), (an extension of the Ciphertext Policy ABE (CP-ABE)) in the public domain and Key-policy ABE (KP-ABE) in the private domain. However CP-ABE fails when complex access control policies are used.

We have already put forth the suggestion of utilizing the Hierarchical Attribute Set-Based Encryption (HASBE) in place of MA-ABE in the public domain in our paper, [2]. In this paper, we implement the HASBE technique to prove its effectiveness, when compound key structures and complex access policies are incorporated.

II. Related Work

Public Key Encryption or PKE schemes were the primary techniques used for enforcing access control for data stored in third party servers. However these led to high key management overhead. Scalability has also become a major issue. As an improvement, 1 to N encryption schemes were introduced. In ABE, the stored data is encrypted with a set of attributes and only those users who have the proper key structure as specified by the PHR file owner/patient are authorized to decrypt the data. Different variants of ABE schemes have been suggested in [3], [4]. Ibraimi et. al. in [5] suggested CP-ABE and also introduced the idea of private-public domains. Another variant of ABE was used by Akinyele et. al. in [6] to create self-protecting

EMRs. Despite successful implementation of the ABE scheme, they were proven to be not much efficient. The presence of a single trusted central authority led to many complications like the key escrow problem, in case of a corrupt central authority. They can cause bottlenecks and key management problems. The user revocation process was also not given due importance.

The KP-ABE was put forth by Yu et. al. in [4]. The owner/patient encrypts the data and distributes the keys to those who need access to information. Key Management is kept to a minimum because of the limited amount of users. User revocation is also present. It is, however, inefficient in a multi-owner/patient scenario. Lewko and Waters's ABE [7] is a revocable ABE but has high key update communication overhead. MA-ABE, a variant of the CP-ABE scheme, proposed by Chase and Chow in [8] lacks efficient user revocation. Basic CP-ABE schemes are not much effective, when complex access policies are involved. CP-ABE supports the involvement of user attributes that can only be grouped as a single set. Bobba et.al. set forth the suggestion of Ciphertext Policy Attribute Set-Based Encryption (CP-ASBE or simply ASBE) in [9], where user attributes can be grouped into a recursive set structure form, which leads to much greater flexibility in expressing complex access policies, thereby providing more efficiency in barring unauthorized personals from gaining illegal access to information.

ASBE can be used to put into effect restrictions on uniting attributes to satisfy an access policy set by an owner. When recursive structures are used, attributes from the same set can only be grouped to realize a policy while those from different sets cannot be joined. This provides more feasibility in many complex situations. ASBE is also capable of allotting multiple values to the same attribute which helps in solving user revocation. However, ASBE does not support a hierarchy structure of attribute or domain authorities. The HASBE described in [2] is the solution for this scenario. It is an extended version of ASBE and is capable of handling multiple levels of authorities.

III. LITRATURE SURVEY

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:

International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 08
July 2019

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.

IV.SYSTEM OVERVIEW

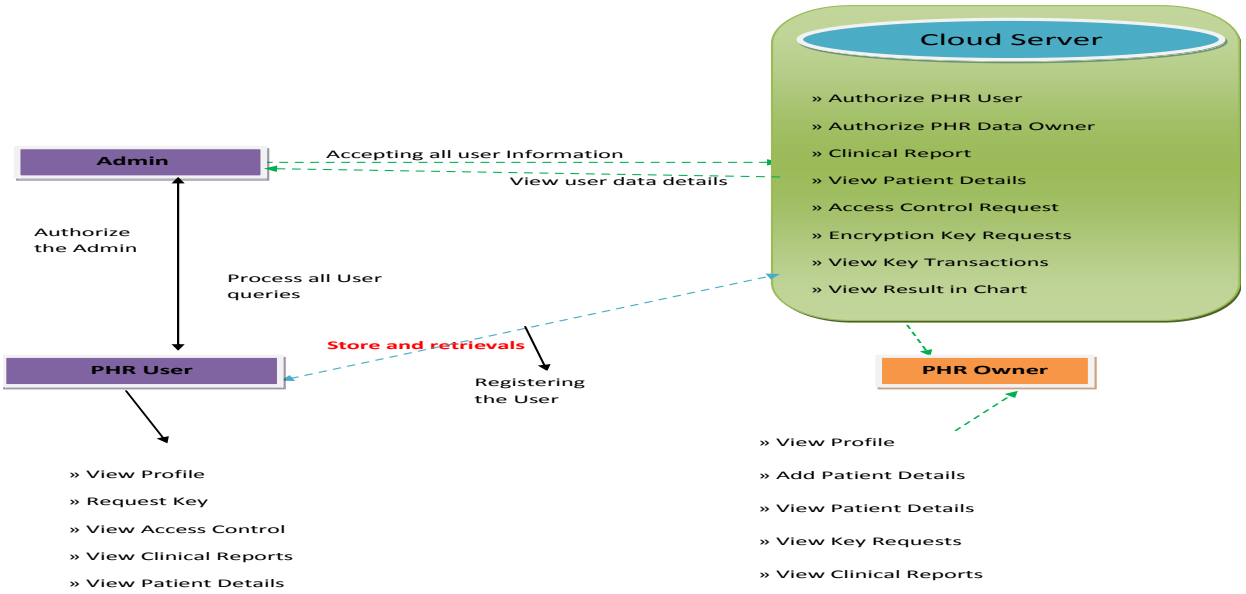

Fig1: Architecture

Cloud Server

In this module, the Server login by using valid user name and password. After login successful he can do some operations such as Authorize PHR User, Authorize PHR Data Owner, Clinical Report, View Patient Details, Access Control Request, Encryption Key Requests, View Key Transactions, and View Result in Chart

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

PHR Owner

In this module, there are n numbers of Owners are present. Owner should register before doing any operations. Once Owner registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful Owner will do some operations like View Profile, Add Patient Details, View Patient Details, View Key Requests, and View Clinical Reports

PHR User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like View Profile, Request Key, View Access Control, View Clinical Reports, and View Patient Details

V. RESULTS AND DISCUSSION

According to proposed survey system provide the highest security of personnel; heath care data in cloud environment.

Advantages

II. System can work any kind of encrypted data without any third party dependency.

ϑϑ. Minimum time complexity.
KK. System can work on big data.
ΛΛ. It can be applicable for structured as well semi structured data.
MM. Can be achieve RBAC for end user.

- There is only single disadvantages for system, searching depends on keyword trapdoor generation, if the some words has generate wrong trapdoor when no background knowledge, then system generate false positive ratio.

- Cloud base encrypted document search system for health care systems on PHR data.
- Encrypted document verification system for banking applications.
- Role base access control applications on public cloud system.
- Document search on encrypted with multi keyword search applications.

VI. CONCLUSION

Data security is the major problem in cloud storage. Before outsourcing PHR into the third party server different attribute based encryption schemes are used for secure storage. ABE is used 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 affiliation. Using Enhance MA ABE scheme, better on demand revocation is possible. In practical case some more problems will arise. The main issue in this case is trying to implement work flow based conditions. For solving these need attribute-based broadcast encryption (ABBE). Work flow Based situation is implement using ABBE and analyze security and computation cost. From analysis show that this work flow based scheme is both scalable and efficient. It gives better on demand user revocation also.

VII. FUTURE WORK

In future it would be interesting to consider Attribute Based Broadcast Encryption system with different types of impressibility. If consider different credential are equal then Distributed ABE scheme is needed.

REFERENCES

[1] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility with Pairing-Based Cryptography," IEEE Access, 2017.

[2] M. Marwan, A. Kartit, and H. Ouahmane, "Protecting medical data in cloud storage using faulttolerance mechanism," in Proceedings of the 2017 International Conference on Smart Digital Environment, 2017, pp. 214–219.

[3] A. Galletta, L. Bonanno, A. Celesti, S. Marino, P. Bramanti, and M. Villari, "An approach to share MRI data over the Cloud preserving patients' privacy," in Computers and Communications (ISCC), 2017 IEEE Symposium on, 2017, pp. 94–99.

[4] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, 2010, pp. 268–275.

[5] K. Shah and V. Prasad, "Security for Healthcare Data on Cloud," 2017.

[6] S. Supriya and S. Padaki, "Data Security and Privacy Challenges in Adopting Solutions for IOT," in Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on, 2016, pp. 410–415.

[7] A. Ibrahim, B. Mahmood, and M. Singhal, "A secure framework for sharing Electronic Health Records over Clouds," in Serious Games and Applications for Health (SeGAH), 2016 IEEE International Conference on, 2016, pp. 1–8.

[8] P. Metri and G. Sarote, "Privacy issues and challenges in cloud computing," Int. J. Adv. Eng. Sci. Technol., vol. 5, no. 1, pp. 5–6, 2011.

[9] Washington Electronic Authentication Act, "Revised Code of Washington," Vol RCW, vol. 70, no. 10, 1992.

[10] P. Duquenoy, N. M. Mekawie, and M. Springett, "Patients, trust and ethics in information privacy in eHealth," in eHealth: Legal, Ethical and Governance Challenges, Springer, 2013, pp. 275–295.

Author's Profile:

CHINDRIPU. JEMERIS CHERIAN Studying M.Tech (2nd year Pursuing) Computer Science and Engineering.

S.Chittibabulu Working as Associate Professor Qualification:M.Tech(Ph.D)