A Review Paper on Privacy Based Secure Sharing of PHR in the Cloud using Encryption

Puja M Tambe
Department of Computer Engineering
Vishwa bharti College of Engineering,
Ahmednagar

Prof. Nisar S Shaikh
Department of Computer Engineering
Vishwa bharti College of Engineering,
Ahmednagar

***Abstract*: The health information exchange, which is often stored at cloud servers need to be secured from malicious attacks. PHR which is personal health record in Hosiptals need to be stored, shared and used by different hospital staff be. To guarantee security of the patients record a 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 development, a model and mechanism to control of data access to PHRs stored in cloud servers are done by doctors itself. To achieve efficient and modular data access control for PHRs, we provide AES encryption approach to encrypt each PHR file and to view use reencryption technique. 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. 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.**

Keyword: Encryption, PHR, cloud computing,key management.

I. INTRODUCTION

Cloud computing means storing and accessing data and programs over the internet instead of using computer's hardware and soft-ware. Data security is the major problem in cloud computing. For security, different attribute based encryption schemes are used for encryption before outsourcing data to cloud server. Personal Health Record (PHR) service is an emerging model for health information exchange. It allows patients to create, update and manage personal and medical information. Also they can control and share their medical information with other users as well as health care providers. Advance technology of cloud computing PHR has undergone substantial changes. Most health care providers and different vendors related to healthcare information technology started their PHR services as a simple storage service. Then turn them into complicated social networks like service for patient to sharing health information to others with the emergence of cloud computing. PHR data is hosted to the third party cloud service providers in order to enhance its interoperability. However, there have been serious security and privacy issues in outsourcing these data to cloud server. For security, encrypt the PHRs before outsourcing. So many 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. To achieve fine-grained and scalable data access control for client's data, a novel patient-centric framework is used.

We present a methodology called Secure Sharing of PHRs in the Cloud (SeSPHR) to administer the PHR access control mechanism managed by patients themselves. The methodology preserves the confidentiality of the PHRs by restricting the unauthorized users. Generally, there are two types of PHR users in the proposed approach, namely: (a) the patients or PHR owners and (b)the users of the PHRs other than the owners, such as the family members or friends of patients, doctors and physicians, health insurance companies' representatives, pharmacists, and researchers.

The patients as the owners of the PHRs are permitted to upload the encrypted PHRs on the cloud by selectively granting the access to users over different portions of the PHRs. Each member of the group of users of later type is granted access to the PHRs by the PHR owners to a certain level depending upon the role of the user. The levels of access granted to various categories of users are de-fined in the Access Control List (ACL) by the PHR owner. For example, the family members or friends of the patients may be given full access over the PHRs by the owner. Similarly, the representatives of the insurance company may only be able to access the portions of PHRs containing information about the health insurance claims while the other confidential medical information, such as medical history of the patient is restricted for such users.

II. LITERATURE SURVEY

Chu et al.[1] proposed a new public key cryptosystem which can aggregate any set of secret keys to generate a single compact aggregate key encompassing the power of all the keys being aggregated. But the work did not focus on how it can help patients to have fine grained access control and revocation of access control and at the same time ensuring confidentiality, authentication and integrity of their PHRs.

Kuo et al. [2] proposed a scheme for patient-centric access control over PHR data. The proposed scheme ensures the following security properties: (1) confidentiality of health data, (2) integrity of health data, (3) authenticity of health data, (4) patient-centric fine-grained access control, and revocation of access control using symmetric key cryptosystem and proxy re -encryption (PRE) scheme. But the main drawback of this scheme is, each file category is encrypted with distinct secret key so whenever a data user (e.g. Doctor or nurse) wants to update PHR categories, patient have to provide the corresponding secret keys. Besides this, the scheme is based on proxy re-encryption scheme which requires data owners to have too much trust on the proxy that it only converts cipher texts according to his instruction. A PRE scheme allows data owners to delegate to the proxy the ability to convert the cipher texts encrypted under his public key into ones for data users. Hence it is desired that proxy doesn't reside in the storage server. This increases communication overhead since every decryption requires separate interaction with the proxy.

So in this paper, we redesign the scheme in [2] for patient-centric access control over PHR data belonging to the patient using the concept of a key-aggregate cryptosystem. Our solution ensures the following security properties: (1) confidentiality of personal health data, (2) integrity of personal health data, (3) authenticity of personal health data, (4) patient -centric fine-grained access control, and (5) revocation of access control.

Chen et al. [4] proposed an EHR solution, relying mainly on smart cards and RSA that enables patients to store their medical records on hybrid clouds. In this approach, patients' medical records are stored in two types of cloud: the hospital's private cloud and the public cloud. The authors discussed two usage cases. The first is that of the medical records being accessed by the owner of the data, i.e., the doctor who created the records. They can directly access the records from their private cloud or from the public cloud.

The second case is that of the medical records being accessed by other hospitals, who must seek permission from the data owner before they can access the records. The authors also provide a solution for emergency situations. However, the shortcoming of this approach is that data owners, i.e., doctors have access control for the medical records and their computing load is heavy.

Leng et al. [5] proposed a solution that allows patients to specify a policy to support fine -grained access control. They primarily utilized Conditional Proxy Re-Encryption to enforce sticky policies and provided users with write privileges for PHRs. When users finish writing data to their PHRs, they sign the modified PHRs. However, users sign the PHRs using the signature key of the PHR owner and it is therefore difficult to correctly verify who signed the PHRs.

III DISADVANTAGES OF EXISTING SYSTEM

- Patient not able to upload data properly in encryted form
- As patient centric control result in data theft by user and doctor not able to receive file on time
- Doctor is responsible to know pateint history disesase related to him and needs to maintain record for further reference.
- So there is no security provided on doctor side and hospital management
- Hospital staff should access part of user data and not pateint record completely but this is not managed in existing system
- Pateint have access control over data but in case if staff ask for PHR data and this could be phishing and spooking attack were pateint doesn't know about it.
- Also access control and key management is having problem in existing system.
- Proposed system: This system make doctor centric control.
- Doctors are responsible to share patient record to staff approved by them this will prevent from unauthorized access
- Hospital will authorize particular doctor to patient on pateint query or disease this will be in it's domain
- Patient will only need to get appointment from staff and contact particular doctor
- Doctor will upload encryted data and keep record safe.
- The other copy will be maintain by Hosiptal in encryted form .
- Patient will be able to download view edit PhR and able to share from his end
- Cloud server will able to maintain encryted record and provide a key to staff on authorization.

III. PROPOSED SYSTEM

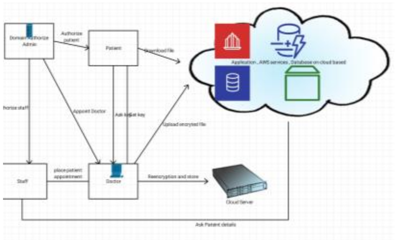

Fig 1. System architecture

Block Description:

2.1 (Patient) PHR Owner Module: The PHR Owner module provides 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. This is patient registration module where details of patient provided and also suitable doctor is assigned to it. It also gives access control by requesting and distributing keys to different users.

2.2.2 Server Module: The server is semi-trusted. The system assumes each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols. In the framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users.

2.2.3 Data confidentiality Module: The owners upload AES encrypted PHR files to the server. For encryption of AES algorithm and MD 5 technique is used for key generation technique is used for Encryption.

2.2.4 Doctor (PHR User): This module takes user registration as doctor and assigned to patient on server authentication it can view patient file only on request granted and also provide prescription to patients based on it. Appointments are fixed and assigned to each patient are authorized.

2.2.5 Receptionist (PHR user) : This module provides appointment to doctor from patient. And have limited access to the data of patient .This shows how PHR system divided in different users but with separate domain access to each user.

2.2.6 Cloud: 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.

Algorithm:

1. Patient makes registration with email password phone and disease caused. 2. Admin or owner whenever makes login check the new user and activate them or deactivate them.

3. Doctor makes registration with email phone and specialization.

4. Admin or owner whenever makes login check the new user and activate them.

5. Patient is able to make login and update profile .

6. Patient makes request for appointment and submit details for doctor.

7. Receptionist makes registration and login.

8. Receptionist forward request to the doctor makes appointment fix.

9. The particular doctor is activated by admin and on login of that doctor is able to see request and

patient disease

10. Then doctor uploads the file record of that patient in encrypted form.

11. Also precipitation is given to requested patient.

12. On patient login the file is download on key request.

13. If user is authenticated then email and text is sent of key for decryption.

14. user can now download file with key.

15. Analyses and prediction is seen by doctor login for more research and survey purpose

AES

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 n encrypted

format. AES allows for three different key lengths: 128, 192, or 256 bits.

IV. ACKNOWLEDGMENT

I wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally I wish to thank to all our friends and well-wishers who supported us in completing this paper successfully I am especially grateful to our guide for him time to time, very much needed, valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

V. CONCLUSION

With the increasing popularity of modern healthcare systems based on cloud storage, how to protect PHRs stored in the cloud is a central question. Cryptographic techniques are getting more versatile and often involve multiple keys for a single application which increases the key management overhead. In this article, also discuss how the confidentiality, and authentication of PHRs can be achieved using a key aggregate cryptosystem. This system also enables a patient to exercise complete control over their PHRs and perform revocation of access rights.

REFERENCES

[1] C. Chu, S. Chow, and W. Tzeng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25 (2): 468- 477.

[2] Kuo-Hsuan Huang, En-Chi Chang, and Shao-Jui Wang, "A Patient-Centric Access Control Scheme for Personal Health Records in the Cloud", Fourth International Conference on Networking and Distributed Computing, 2014.

[3] Dixit, G. N. “Patient Centric Frame Work For Data Access Control Using Key Management In Cloud Server”, International Journal of Engineering, 2 (4), 2013.

[4] Chen, Y. Y., Lu, J. C., & Jan, J. K. “A secure EHR system based on hybrid clouds,” Journal of medical systems, 36 (5), 3375 - 3384, 2012.

[5] Leng, C., Yu, H., Wang, J., & Huang, J. “Securing Personal Health Records in the Cloud by Enforcing Sticky Policies,” TELKOMNIKA Indonesian Journal of Electrical Engineering, 11 (4), 2200-2208, 2013.

[6] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records”, Proc. ACM Workshop Cloud Computing Security (CCSW 09), pp. 103 -114, 2009.

[7] Chen Danwei, Chen Linling, Fan Xiaowei, He Liwen, Pan Su, and Hu Ruoxiang “Securing Patient-Centric Personal Health Records Sharing System in Cloud Computing”, China Communications, Supplement No.1, 2014.

[8] Ming Li, Shucheng Yu, and Yao Zheng, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption”, IEEE Transactions on Parallel and Distributed Systems, 24(1), pp. 131-143, 2013.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data”, Proc. 13th ACM Conf. Computer and Comm. Security (CCS 06), pp. 89-98, 2006.

[10] M. Chase, and S.S.M. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption”, Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009.

[11] R. Canetti, and S. Hohenberger, “Chosen-Ciphertext Secure Proxy Re- Encryption”, Proc. 14th ACM Conf. Computer and Comm. Security (CCS 07), pp. 185-194, 2007.