Preserving The Privacy Of Patient Health And Monitoring Over The Cloud

S.Sivagnanam
Department of CSE
Francis Xavier Engineering College
sivagnanamcse15@gmail.com

P.ThambiranThozhan
Department of CSE
Francis Xavier Engineering College
pthambiranthozhan@gmail.com

Mrs.P.Brundha
Head of Department/CSE
Francis Xavier Engineering College

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 then 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 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.Furthermore, we formally analyze and verify the working of SeSPHR methodology through the High Level Petri Nets (HLPN).

Keywords: Access control, cloud computing, Personal Health Records, privacy

1. INTRODUCTION

In the proposed research work to design and implementa system that can provide the security to Personnel Health Records (PHR) files using semi trusted proxy re- encryption services, and eliminate the insider attacks like collusion attack, bruited force attack as well as SQL injection attack. In this research work to design and implement a security and privacy mechanism health care system such as, data confidentiality, data integrity and fine grained access control. The privacy and security are most common issue in the cloud environment. In this architecture clouds are used with some advantages like a huge storage capacity and high scalability. The used Attribute Based Encryption (ABE) algorithm for the fine grained access control. The attribute based encryption algorithm first encrypt data before storing it on the cloud server. In ABE there are two variants based on placing attributes and access attribute policy. 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.

2. EXISTING SYSTEM

Although cloud-assisted mHealth monitoring could offer a great opportunity to improve the quality of healthcare services and potentially reduce healthcare costs, there is a stumbling block in making this technology a reality. Without properly addressing the data management in an mHealthsystem, clients' privacy may be severely breached during the collection, storage, diagnosis, communications and computing. This privacy concern will be exacerbated due to the developing trend in privacy breaches on electronic health data. We first find the design problems on privacy preservation and then provide our solutions. To ease the understanding, we start with the basic scheme so that we can identify the possible privacy holes.

2.1.Disadvantage:

The resulting improved scheme allows the mHealth service provider (the company) to be offline after the setup stage and enables it to deliver its data or programs to the cloud securely. It is based on a new variant of key private proxy re encryption scheme, in which the

company only needs to undertake encryption once at the setup phase while shifting the rest computational tasks in the cloud without compromising privacy, further reducing the computational and communication burden on clients and the cloud.

3. PROPOSED SYSTEM

In the proposed research work to design and implement
a system that can provide the security to Personnel Health Records (PHR) files using encryption as well as proxy re-encryption services, in cloud environment and provide the security from insider attacks like collusion attack, bruited force attack as well as SQL injection attack.

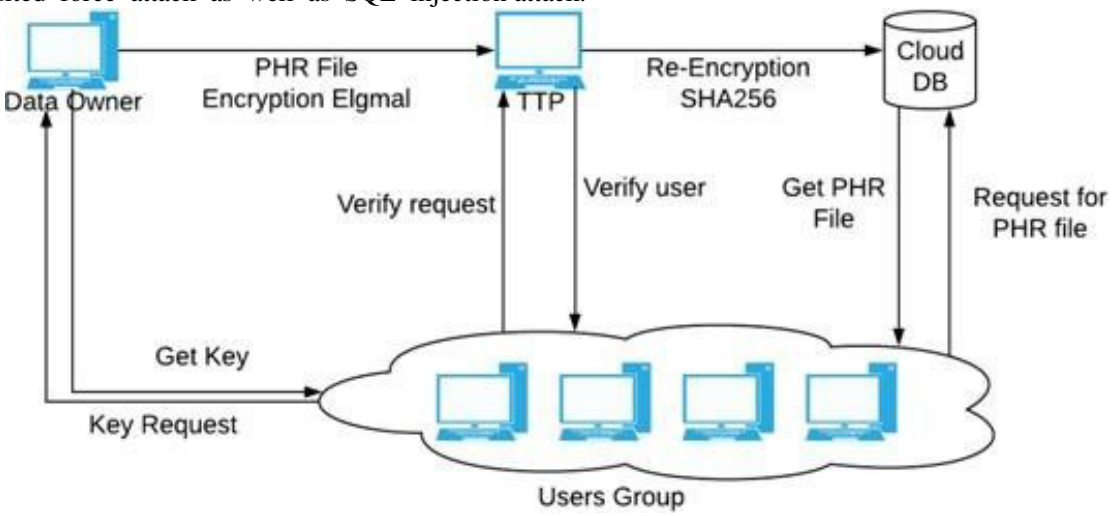

Figure 1 : Proposed System Architecture

In this architecture the will give some security and privacy mechanism such as, confidentiality, data integrity and fine grained access control. The privacy and security are most common issue in the cloud environment. In this architecture clouds are used with some advantages like as a huge storage capacity and high scalability. The used Attribute Based Encryption (ABE) algorithm for the fine grained access control. The attribute based encryption algorithm first encrypt data before storing it on the cloud server. In ABE there are two variants based on placing attributes and access attribute policy. The system first upload the own PHR file on cloud using Elgamal encryption scheme. This file first received by TTP and generate the proxy re-encryption using SHA-256 algorithm and store the file into the cloud server. Data owner can share the file to individual user as well as whole group using RBAC algorithm. When end user's give request to CSP, then authentication has done by TTP. In the proposed work we have written web service for owner that can 24*7 available for private key distribution. When data owner revoke any user system automatically expired the existing keys and generate new keys.

4. RESULTS AND DISCUSSION

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

4.1. Advantages:

System can work any kind of encrypted data without any
third party dependency. It has minimum time complexity. System can work on big data. It can be applicable for structured as well semi structured data. It can achieve RBAC for end user.

4.2. Disadvantages:

There is only single disadvantage 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.

4.3. Applications:

Cloud base encrypted document search system for health

care systems on PHR data. It provides 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.

5. CONCLUSION

Data security is the major issue 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 request 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 analysisshow that this work flow based scheme is both scalable and efficient.

6. REFERENCES

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

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

[3] A. N. Khan, ML M. Kiah, S. A. Madani, M. Ali, and S. Sham- shirband, "Incremental proxy re-encryption scheme for mo- bile cloud computing environment," *The Journal of Supercom- puting*, Vol. 68, No. 2, 2014, pp. 624-651.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- sharing (CollaborateCom), 2012, pp. 711-718.

[4] 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.

[5] 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 Comput- er and System Sciences, vol. 90, pp, 46-62, 2017.

[6] J. Li, "Electronic personal health records and thequestion of privacy," Computers, 2013, DOI:
10.1109/MC.2013.225.

[7] 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.

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

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

[10] 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.

[11] K. Gai, M. Qiu, "Blend arithmetic operations on tensor-based fully homomorphic encryption over realnumbers," IEEE Transactions on Industrial

[12] 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.

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

[14] Z. Xiao and Y. Xiao, "Security and privacy in cloud compu- ting," IEEE Communications Surveys and Tutorials, vol. 15, no. 2, pp. 1–17, Jul.2012.

[15] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in Proceedings of CRYP- TO 84 on Advances Cryptology,1985, pp. 10-18.

[16] W. Diffie, and M. E. Hellman, "New directions in cryptog- raphy," IEEE Transactions on Information Theory, vol. 22, no. 6, 1976, pp.644-654.

[17] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L.Alem, "A platform for secure monitoring and sharing of generic health data in the Cloud," Future Generation Computer Systems, vol. 35, 2014, pp. 102-113.

[18] S. U. R. Malik, S. U. Khan, and S. K. Srinivasan, "Modeling and Analysis of State-of-the-art VM-based Cloud Manage- ment Platforms," IEEE Transactions on Cloud Computing, vol. 1, no. 1, pp. 50-63, 2013.