ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015.

Scalable and Secure Sharing of Personal Health Records in centralized Database Using Attribute-based encryption

Prof.:-KanchanHadawale, NikamManoj B[1], KadamJayesh D[2], Salgar Vijay L[3], GhogareSagar R[4]

Computer Engineering, Sharadchandra Pawar College of Engineering Dumbarwadi (Otur), Junnar, Pune, India[1,2,3,4]

Abstract: Personal health record (PHR) is used to maintain patient's personal and diagnosis information, and is stored at a thirdparty i.e., cloud providers. The main concern is about diagnosis information. Due to Personal health record (PHR) patient manage and create his its own health record and the patient's could actually control the sharing maintain with high security and high privacy. Personal health record (PHR) protect and secure the patient's personal health information (PHI) from unauthorized users. The patient's have control over access to their own PHR. To achieve high security of personal health records, we use the attribute based encryption technique to encrypt the all patient's data before outsourcing or before access from unauthorized user. We prestige attribute-based encryption (ABE) practices to attain scalable and fine grained data access control for personal health records to encrypt each patient's PHR file. Data owner update the personal health data into third party cloud data centers. Multiple data owners can access the same type of patient's data from cloud. The Personal health record (PHR) is a high degree of patient's privacy is guaranteed.

Keywords: Personal health records (PHR)**,** Personal health information (PHI), Attribute-based encryption (ABE), data privacy, fine-grained access control.

I. INDRODUCTION

Personal Health Record (PHR) is emerged as a patient-centric model of health information exchange. He can create, delete, modify and share his or her PHR through the web. Due to PHR the patient to create and control their medical data which may be placed in a single place such as data center. The main concern is whether the PHR owner actually gets full control of his data or not, especially when it is stored at third party servers which is not fully confidential. Our aim is to encrypt the data before access from unwanted user it. PHR owner will decide which users will get access the data in his PHR record. A PHR file should available to only those users who have corresponding decryption key to encrypted data. Each patient is full control of his or her medical records and can share his or her health data with wide range of users, including friends, healthcare providers or family members. On the other hand, due to the high value of sensitive Personal Health Information (PHI), the third - party storage servers are often the targets of various malignant behaviors which may lead to exposure of the PHI In security based ensure privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. It divides the users in the PHR system into several security domains which decreases the key management complexity for owners and users. Simultaneously, patient confidentiality is maintained and guaranteed by exploiting multi authority ABE.

II. PROPOSED SYSTEM

We need to use attribute-based encryption (ABE) techniques to achieve scalable and secure data access control for personal health records to encrypt each patient's PHR file.

In this paper we concentrate on the multiple data owner condition, which is different from previous works in secure data outsourcing. It divides the users in the PHR system into many security domains which decreases the key management complexity for owners and users. We know that the Personal Health Record is the web based application which is allows people's to access a their health information from cloud. There are many different techniques of cryptographic methods like AES, MD5 they provide to guarantee data security. In this work we propose a unique authentication and encryption technique using AES algorithm. In this paper we are providing security to patient's health data or personal health information or medical history.

III. ADVANTAGES OF PROPOSED SYSTEM

1) We can easily find out information of patient's medical history details.
2) In case of emergency, doctor and other emergency department easily get all the informative details and start treatment of patient related to diagnosis.
3) To provide easy and faster access information from cloud.
4) Its user friendly system.

IV. SYSTEM ARCHITECTURUL DIAGRAM

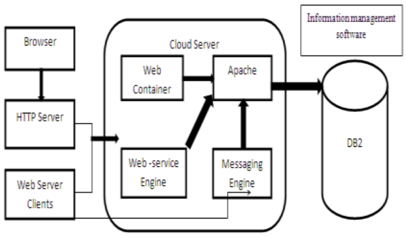

Fig 1. System Architecture.

DOI 10.17148/IJARCCE.2015.43128

V. ATTRIBUTE BASED ENCRYPTION

Using Attribute Based Encryption (ABE) technique we are providing security to the patient's health records and all databases. We are using attribute-based encryption (ABE) as the main encryption technique to secure the data.

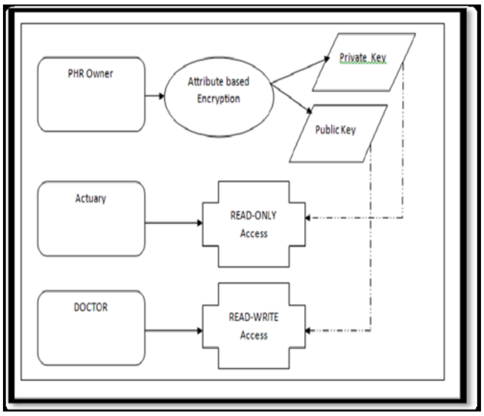

Fig 2: Block Diagram for PHR using attribute based encryption

VI. IMPLEMENTATION DETAILS

Implementation steps:-

1) Setup
2) User Registration
3) Key Generation
4) Encryption
5) Re-encryption
6) Decryption

VII. APPLICATION

1) Any organization can use this application to store their employee's medical information.
2) This application is used to secure the patient's sensitive information.
3) With the help of this application Doctor can easily access the patient health information from cloud server.

VIII. CONCLUSION

Personal Health Records are maintained with security and privacy. In future, to provide high security and privacy for Personal Health Record (PHR).The personal health record system needs to provide security against attackers and hackers. Scalable and Secure sharing includes basic securities to protect the information from unauthorized access and loss. This paper proposed the new approach for existing PHR system for providing more security using attribute based encryption which plays an important role because these are unique and not easily hack able. We are reducing key management problem and also we enhance privacy guarantee.

REFERENCES

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

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

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted personal health records in cloud computing," in ICDCS '11, Jun. 2011.

[4] "The health insurance portability andaccountability 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] K. D. Mandl, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private," BMJ, vol. 322, no. 7281, p. 283, Feb. 2001.

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

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEEINFOCOM'10, 2010.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of ComputerSecurity, 2010.

BIOGRAPHIES

Sagar R. Ghogare, Department of Computer Engineering, Sharadchandra Pawar Collage of Engineering at the Savitribai Phule Pune University, HSC in 2009, Maharashtra State Board Pune, sagarghogare8@gmail.com

Vijay L. Salgar, Department of Computer Engineering, Sharadchandra Pawar Collage of Engineering at the Savitribai Phule Pune University, HSC in 2010, Maharashtra State Board Pune, salgarvijay@gmail.com.

Jayesh D. Kadam, Department of Computer Engineering, Sharadchandra Pawar Collage of Engineering at the Savitribai Phule Pune University, HSC in 2010, Maharashtra State Board Pune, jayeshkadam103@yahoo.com.

Manoj B. Nikam, Department of Computer Engineering, Sharadchandra Pawar Collage of Engineering at the Savitribai Phule Pune University, HSC in 2010, Maharashtra State Board Pune, nikam.manoj@gmail.co

DOI 10.17148/IJARCCE.2015.43128