International Journal on Applications in Engineering and Technology
Volume 5 : Issue 1: December 2019, pp 1 – 4 www.aetsjournal.com ISSN (Online) : 2455 - 0523

SECURE AND EFFICIENT PERSONAL HEALTH RECORD SHARING IN CLOUD COMPUTING

P.BHUVANESHWARI , G.NIVEDHITHA , Dr. E. PUNARSELVAM

Abstract — Personal health record is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the personal health records before outsourcing. Some 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 PHRs, the new system is leverage attribute based encryption techniques to encrypt each patient's personal health records file. Different from previous works in secure data outsourcing, developer focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. The new scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of the proposed scheme.

Key Terms: Access control, cloud computing, Personal Health Records, privacy.

I. INTRODUCTION

The personal health record has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control person personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of patient medical records and can share the health data with a wide range of users, including healthcare providers, family members. Because of high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third party service providers.

P.Bhuvaneshwari , Assistant Professor , Department of Information Technology , Muthayammal Engineering College.

G.Nivedhitha , Assistant Professor , Department of Information Technology , Muthayammal Engineering College.

Dr. E. Punarselvam , Associate Professor , Department of Information Technology, Muthayammal Engineering College.

II. RELATED WORKS

1) Confidentiality of PHD,

Before uploading a health record, it is encrypted using the product of public key and Minimum Shift Keying. The master secret key is kept secret. When patient generates an aggregate key, it is the product of master secret keys, data user or an interceptor cannot obtain each multiplier from the product. Hence, even component of the encryption key is publicly available, other component Minimum Shift Keying is hidden hence confidentiality of personal health data is ensured secure and efficient data sharing scheme also enables a data owner to have full control over PHR

2) Authenticity of PHD

The owner of the PHR generates an aggregate key. At the time of decryption, an aggregate key successfully decrypts the authorized set of cipher text. This verifies the authenticity of personal health data. Each owner's PHR file encrypted both under a certain fine grained model. Data owner (patient) encrypts different categories of personal health records with different keys and sends the corresponding secret keys to data users like doctors, nurses, relatives etc.

3) Patient-centric access control

The PHR owner generates a value representing a particular access right while generating the aggregate key. The PHR owner can control access privileges for every user. The sharing of PHRs and introduced the concept of social/professional domains investigated using ABE to generate self-protecting EMRs that can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline.

4) Revocation of access control

If the PHR owner wishes to revoke some users in a certain category then the user need only to replace the aggregate key Ks with Ks1. The small aggregate key size minimizes the communication for transferring the new key. Access privileges for fine-grained access control of the PHR data, PHR data categories should be accessible only to those users possess the corresponding decryption keys and the set of decryption keys should be kept confidential from others with the minimum key management overhead. The solution employs the concept of a key aggregate cryptosystem and successfully resolves the problem of data access control in a health care setting

III. PROPOSED SYSTEM

To enable fine-grained and scalable access control for PHRs, leverage attribute based encryption techniques to encrypt each patient's PHR data. To reduce the key distribution complexity, divide the system into multiple security domains that each domain manages only a subset of the users. Our PHR sharing system consists of the following five parts: health care provider, cloud service provide, trusted central authority domain authority, lower level attribute authority, PHR data owner and PHR user. Personal health record enables patients to manage the patient's own electronic medical records in a centralized way, and it is often outsourced to be stored in a third-party server.

The purpose of secure and scalable system is sharing PHRs. It focuses on the multiple data owner scenario, and divide the users in the system into multiple security domains that greatly reduce the key management complexity for owners and users.

The main aspect of this framework is to provide protected patient-essential PHR access and useful key management together. Here the goal is to divide the PHR system into different security concern namely, public domains & personal domains according to the various user's data access requirements. In both types of security concerns, utilize ABE to understand cryptographically reinforce, patient-essential PHR access. Specially, in a PUD multi authority ABE is used. Each data owner is a credible authority of his own PSD, data owner uses a KP-ABE system to maintain the secret keys and access authority of users in his PSD.

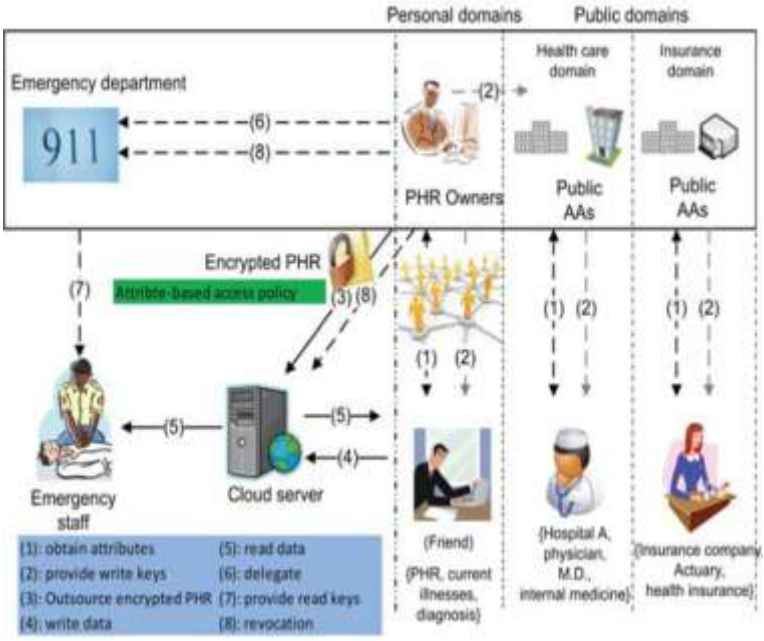

Figure 1 : System Architecture

IV. ALGORITHM

Algoithm 1: Top-Range Computation
Input :[d'_0,d'_{n+1}],n,k,c
Output:[d'_0,d'_n]
1 low:=d'_0; high :=d'_{n+1};
2**while** low≤ high **do**
3 M=(low+high)/2;
4 P= m-d'_0
d'_{n+1}-d'_0
5 $f(d')=\sum^{k-1}_{j=0}(^n_j)p^j(1-p)^{n-j}$;
6 **if** $f(d') \le c$ **then**
7 high :=m-1;
8 **else**
9 low :=m+1;

10 $d^{'}$:= low;
11 **returen** [$d^{'}_{0}$,$d^{'}$]

V. VERIFICATION OF PROPERTIES

To determine whether the presented SeSPHR scheme operates according to the specifications, we performed verification of the properties. The following properties pertinent to the working of SeSPHR methodology are verified:

- A valid system user cannot obtain the re-encryption parameters for a PHR partition for which access is not granted to theuser.
- The encryption and decryption is performed correctly as specified by thesystem.
- Any unauthorized user is not able to generate the re-encryption parameters and decrypt the PHR.

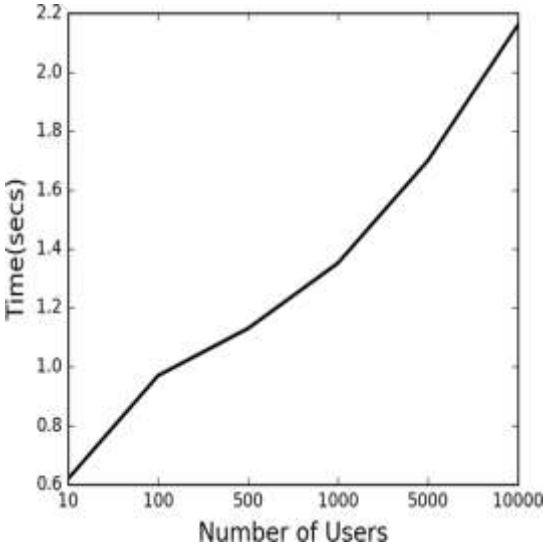

Figure 2

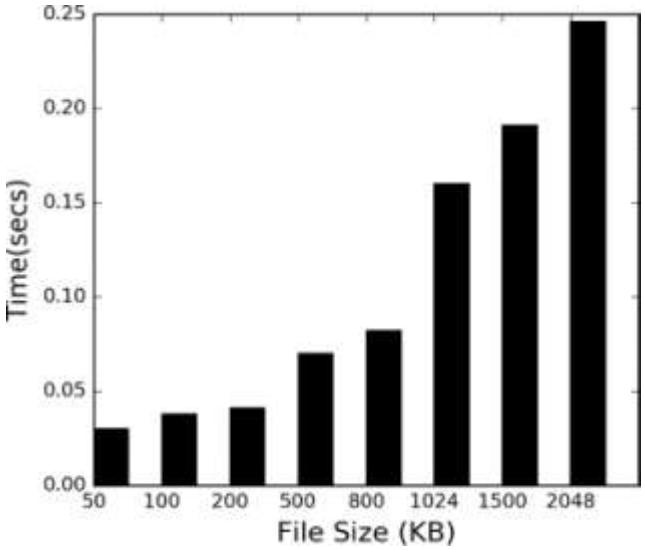

Figure 3

VI. PERFORMANCEEVALUATION

To evaluated the performance of the SeSPHR methodol- ogy from multiple perspectives, such as key generation times, encryption and decryption time, and turnaround time. Also, we compared the complexity of the SeSPHR methodology with other methodologies. The details of the experimental setup and results are presented in sub- sequent sections.

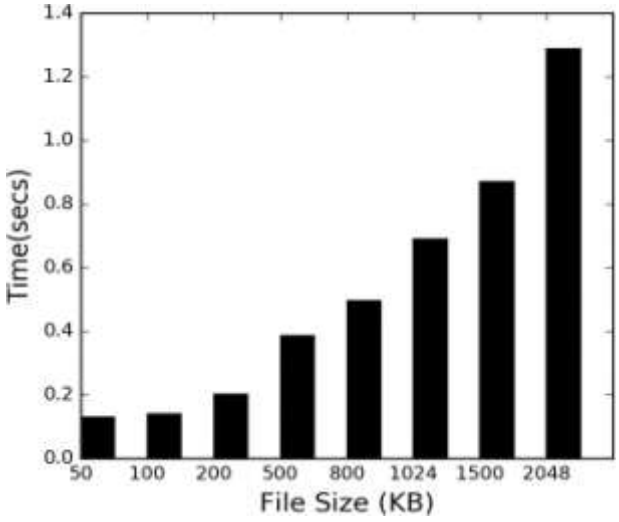

Figure 4

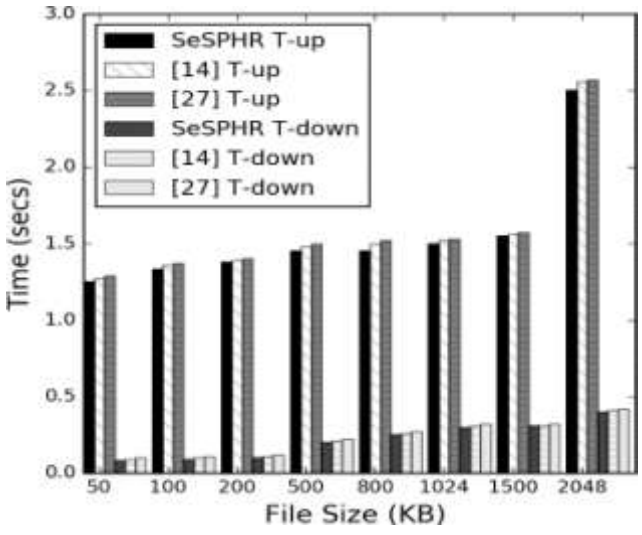

Figure 5

VII. RESULTS AND ANALYSIS

The performance of the SeSPHR methodology was evaluated regarding generation, encryption, decryption, and turnaround time.not the false positive rate introduced by bloom filters[5]. The experimental results show that our proposed scheme

can control the false positive rates to a practically acceptable range.

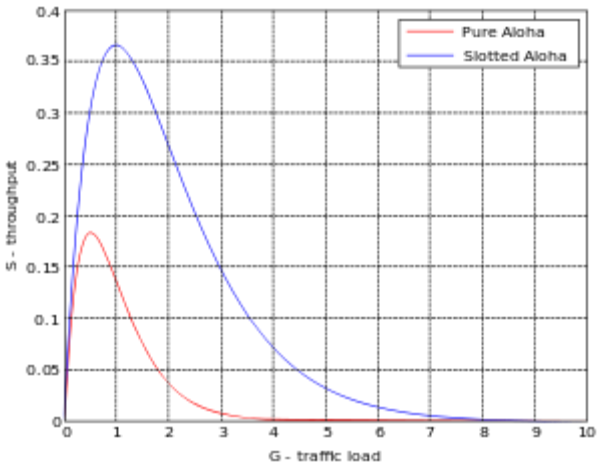

Figure 6 : comparing bandwidth

VIII.KEYGENERATION

As stated earlier in Section 3 that the responsibility of the SRS is to generate the private/public key pairs for the users belonging to the set of authorized users. However, the key generation time for the systems with large num-bers of users may affect the overall performance of the system. Therefore, we appraised the performance of the SeSPHR in terms of the time consumed for the key gener ation step for different number of user. The time consumption for generating keys for 10, 100, 500, 1000, 5000, and 10,000 users in presented .

IX. CONCLUSION

The proposed system , To securely store and transmission of the PHRs to the authorized entities in the cloud. The methodology preserves the confidentiality of the PHRs and enforces a patient-centric access control to different portions of the PHRs based on the access provided by the patients. To implemented a fine-grained access control method in such a way that even the valid system users cannot access those portions of the PHR for which they are not authorized. The PHR owners store the encrypted data on the cloud and only the authorized users possessing valid re-encryption keys issued by a semi- trusted proxy are able to decrypt the PHRs. The role of the semi-trusted proxy is to generate and store the public/private key pairs for the users in the system. In addition to preserving the confidentiality and ensuring patient centric access control over the PHRs, the methodology also administers the forward and backward access control for departing and the newly joining users, respectively. Moreover, we formally analyzed and verified the working of SeSPHR methodology through the HLPN, SMT-Lib, and the Z3 solver. The performance evaluation was done on the on the basis of time consumed to generate keys, encryption and decryption operations, and turnaround time. The experimental results exhibit the viability of the SeSPHR methodology to securely share the PHRs in the cloudenvironment.

References

[1] Ali Gholami and Erwin Laure,“Security and privacy of sensitive data in cloud computing:survey of recent developments”,2018.

[2] Assad Abbas, SameeU.Khan,“A review on the State of the art privacy preserving approaches in the e-health clouds”,2014.

[3] Abdul Nasir Khan1,M.L.Mat Kiah1,Sajjad A.Madani2,“Atta urRehman Khan1,Samee U.Khan3,“A study of incremental cryptography for security schemes in mobile cloud computing environments“2013.

[4] Chia-hui Liu, Tzer-Long Chen,Han-Yu Lin,“Secure PHR Access Control Scheme in cloud computing”,2012.

[5] Qiwei Han, MengxinJiy, I nigoMart´ınez de Rituerto de Troya, ManasGaurz, LeidZejnilovic,“A Hybrid Recommender System for Patient-Doctor Matchmaking in Primary Care”, 2018.

[6] RouyuWul, Gail-JoonAhn, Hongxin Hu,“Secure sharing of electronic health records in clouds”,2012.

[7] Supriya D.Patil , Komal S.Talekar2, Reshma M.Raskar3, Pooja A. Chavans4, Prof Rupali Kadu5,“Attribute based access control in personal health records using cloud computing”, 2016.

[8] Shachindra Kumar Dubey,Prof.Ashok Verma,“Security and privacy in cloud computing”.2016.

[9] Saif Ur Rehman Malik, sudarshan K. Srinivisan, SameeU.Khan, Lizhe Wang,“A Methodology for OSPF Routing Protocol Verification”.2012.

[10] Whitfield Diffie and Martin E .Hellman,“New Directions in Cryptography”2017

.