Journal of Computer Science and Applications.
ISSN 2231-1270 Volume 7, Number 1 (2015), pp. 21-28
© International Research Publication House
http://www.irphouse.com

On Demand Security For Personal Health Record In Cloud Computing

V. Indhumathi [1] and V. Prakasham [2]

*ME – 2nd year Student, Dept of Computer Science & Engg,
Pallavan college of Engineering, Kanchipuram,
Email:mmaddy. indhu@gmail. com
Faculty of Computer Science & Engg,
Pallavan college of Engineering, Kanchipuram,
Email: vprakashamcse@gmail. com*

Abstract

Cloud computing is used broadly in several services that maintain Personal Health Record (PHR). It is a patient health-centric model for data exchange in cloud. Personal Health Record (PHR) is often keeping in a third party server i. e. cloud server. The major problems raised in existing approaches are fine–grained access, cryptographically access control, measurability in key management and effective on-demand user revocation. We would like to provide the secure sharing of patient health information in PHR data. This paper predominantly considers the multi-owner scenario and divides the user in PHR system into multiple security domains that greatly reduces the key management issues. A high degree of patient privacy is enriched at the same time by developing Multi-Authority Attribute based mostly cryptography (MA-ABE). We have to improve the security of Personal Health information and set access privileges for every PHR data. Before taking a key to decipher the PHR record in multiple owner scenarios it must raise some security queries on PHR owner.

Keywords: Cloud Computing, Fine-grained access control, Public Health Record System, Attribute Based Encryption, data privacy, Multi-Authority Attribute Based Encryption, AES File Encryption.

I. INTRODUCTION

Personal Health Record (PHR) concept has emerged in recent years for secure sharing of patient-centric model of health information in cloud. We can say that it is a patient centric model as overall control of patient's data is with patient. Patient can create, delete, modify and share own PHR information through the public cloud and we made to storage, retrieval, then more efficient for sharing of the medical information. Each patient is having the full access control of own Personal Health Information and can share our health data with a wide range of users in public and personal domains. Before providing the PHR data to cloud it must be in encrypted format and feasible approach. The each data should be stored in third-party service and it's provide the PHR service by cloud with many security and privacy risks for Personal Health Record [7]. Using ABE, access policies are stated based on the attributes of users or data, which enables a patient to share our PHR data among a set of users by encrypting the file by using encryption algorithm under a set of attributes. The main issues are encryption; key policy and decryption are easily with the number of aspects involved. We proposed a new Patient-centric framework MA-ABE for secure sharing of PHR information in cloud computing environments, under the multi-owner scenario.

To address the key management challenges, we theoretically divide the users in the system into two types of domains, namely public and private domains. Furthermore, the framework implements fine-grained access control, dynamic policy updates, on demand user revocation and provides a break-glass access policy to PHRs data. 1) In the public domain, we use Multi-Authority Attribute Based Encryption (MA-ABE) to improve the scalability, security, on demand use revocation and avoid the key management issues. Attribute Authorities (AA) plays an important role to check the each user roles and attributes. And any other unauthorized users can't be access the whole system. The mechanisms for key distribution and encryption algorithm so that PHR owners can specify modified, fine-grained access policies during file encryption. 2) In the private domain, owners directly assign access privileges for personal users and encrypt a PHR record under its data attributes. Likewise, we tendency to improve the existing format of PHR data into a secure format and set access privileges. Before fetching a key to encrypt the PHR record in multiple owner scenarios it may raise some questions about PHR owner. We also improve the existing system issues like On-demand user revocation, scalability and security.

II. RELATED WORKS

A. *Attribute-Based Encryption (ABE)*

Attribute Based Encryption is the encryption technique which is used to solve the security problems with outdated data. The preliminary model of the Attribute Based Encryption is keys of users and the Encrypted text are combined with the groups of attributes and using exact key only decrypt the cipher text. So there is the match between the cipher text and private as well as attributes. In the later years the Attribute Based Encryption (ABE) is based on one to many approaches [13], i. e. for particular information for many numbers of users, the encryption schemes are evolved. ABE is a crypto system for fine grained sharing of encrypted data [2]. Ming Li et al has presented a paper on "Securing Personal Health Records in Cloud

Computing: Patient-centric and Fine-grained data Access Control in Multi-owner Settings. ”[7]. The Author implement the best technique for handle the many number of users, i. e. it greatly increases the scalability. So, the Attribute Based Encryption technique can be used for securing the patient health record in cloud with multi-owner scenario. Attribute Based Encryption (ABE) is the primary encryption algorithm to achieve the main issues in Fine Grained Access control in cloud. The most sensitive data is patient health information. So if the health data is maintained with the Cloud is good one but we have to provide the number of security for that cloud data [11].

III. EXISTING SYSTEM

B. Attribute-Based Encryption (ABE)

Using attribute based encryption technique we are providing security to the database. A sensitive PHR data is shared and stored on cloud server, PHR data will be encrypted and stored in a third party. In Attribute based encryption encrypted PHR data with set of attribute. Secret key associated with access structure that manages which encrypted text a user is able to decrypt. We are using Attribute-Based Encryption (ABE) as the foremost encryption algorithm.

Using ABE file Encryption algorithm, access policies are specified based on the attributes of data, which permits a patient-centric model to mainly sharing on own PHR data among a set of users by encrypting the file under a set of attributes. The main issues are encryption; key policy and decryption are easily with the number of aspects involved. Still, to integrate ABE into an important PHR system, important issues such as key policy, scalability, security, and efficient on-demand user revocation are hard to solve.

IV. ALGORITHM

C. Advanced Encryption Standard (AES)

AES is stands for Advanced Encryption Standard. AES is mainly considered for substitution and permutation network. AES is used for transmission of information that is personal health data in encrypted secure format and also it fast in both of software and hardware. AES is basically sending user authentication data in encrypted with secure format. Advanced Encryption Standard (AES) allows for three different key sizes such as: 128, 192, or 256 bits. In our system by encryption we using, each specified round consists of the bellow four steps are: 1. S-bytes 2. Shift rows 3. Mix columns 4. Added round keys and then the last step is XO Ring it is the output of the before three steps. And for decryption, each specified round consists of the below four steps such as: 1. Inverse shift rows 2. Inverse S-bytes3. Add round keys 4. Inverse Mix columns. In this the third step which of consists of XO Ring the output of the before two steps.

1) Substitute bytes

This substitute byte consists of using a 16 × 16 search for table to find a substitution byte (S-bytes) for a given byte in the input position array. And also this operation provides the non-linearity for encrypted data. Thus the entries in the lookup table are created by using the concept of multiplies in inverses in GF (28) and it each bit can be scramble to destroy the bit-level correlation surrounded by each byte.

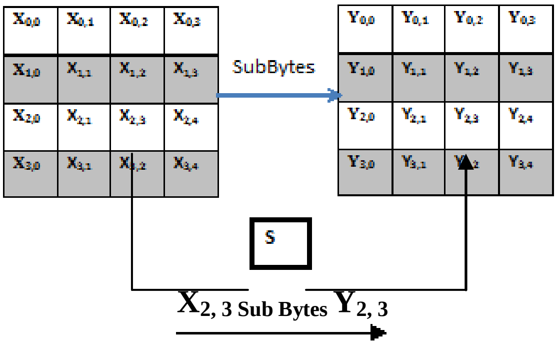

Fig. 1. Shift Sub Bytes in the columns

2) Shift rows

The Shift rows step is mainly operates the rows of the state. For AES, the first row of each left side is not altered. Then the second row is replaced 1 byte to the left side manner. At the same time, the third and fourth rows are replaced by 2 and 3 bytes in left side manner respectively. For each block of sizes 128 bits and 192 bits of pattern are replacing in the same likewise. Row n is replaced left side manner by n-1 bytes.

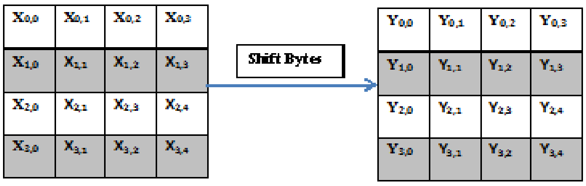

Fig. 2. Shifting bytes in rows

a) *1st row*:no change in first row.

b) *2nd row:* Shift 1

$\mathbf{X_{1,1}} \longrightarrow \mathbf{X_{1,0}}$

$\mathbf{X_{1,2}} \longrightarrow \mathbf{X_{1,1}}$

$\mathbf{X_{1,3}} \longrightarrow \mathbf{X_{1,2}}$

c) *3rd row:* Shift 2

$\mathbf{X_{2,2}} \longrightarrow \mathbf{X_{2,0}}$

$\mathbf{X_{2,3}} \longrightarrow \mathbf{X_{2,1}}$

d) *4th row:* Shift 3

$\mathbf{X_{3,3}} \longrightarrow \mathbf{X_{3,0}}$

Fig. 3. For example shifting of bytes Explained in above diagram

3) Mix columns

In this Mix Column step, the 4 bytes of each column in a state are joined using an invertible linear transformation. The Mix Column function is taken 4 bytes of input and 4 bytes of outputs. During Mix column operation each column is multiple by a fixed matrix.

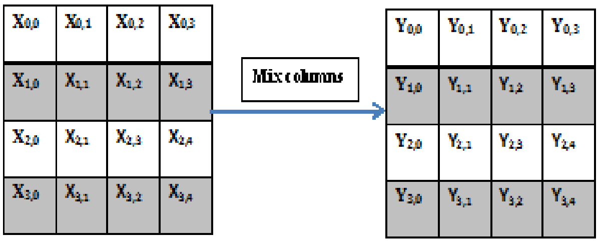

Fig. 4. Mix columns

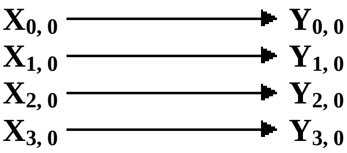

Fig. 5. For example mix columns in bytes Explained in above diagram

The corresponding transformation of mix column is during the decryption is denote converse Mix column transformation. And this step shifted by each byte of a column in a function.

4) Add round keys

In this step sub key is joined in to the state. The equivalent stage during decryption is denoted Inverse Add Round-Key for inverse add round key transformation. In this stage, the 128 bits of state are bitwise XORed with the 128 bit of the round key. Thus the operation is mentioned as column wise method between is 4 bytes of state column.

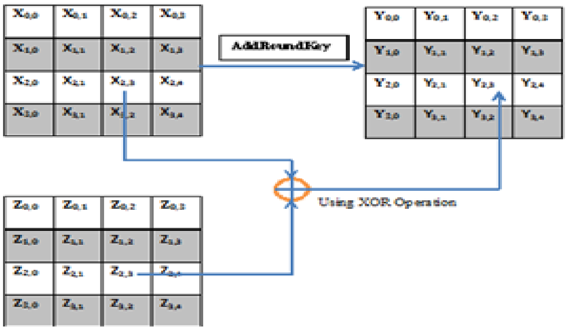

Fig. 5. Add round key using XOR operations.

V. PROPOSED METHOD

D. MA-ABE

The Multi-Authority Attribute Based Encryption scheme is an advanced attribute based encryption it many attribute authority for handling the different set of users from various domains [4]. In the PHR system the users will be from different domain like the doctors from health care organizations, the friends and family other users from insurance domain too. So each user will be having different access control mechanism based on the relation with the patient or the owner. Thus the MA-ABE scheme will highly reduce the key-management issues and overhead and thus it will provide fine-grained access control to the system. In a multi-authority ABE algorithm consists many attribute authorities and many users [3]. In MA-ABE defines a set of public parameters available to everyone (cloud server, or by a distributed protocol between the authorities). A user can choose an Attribute Authority (AA), prove that it is entitled to some of the attributes handled by that attribute authority, and request the corresponding distributed key to decrypt PHR data.

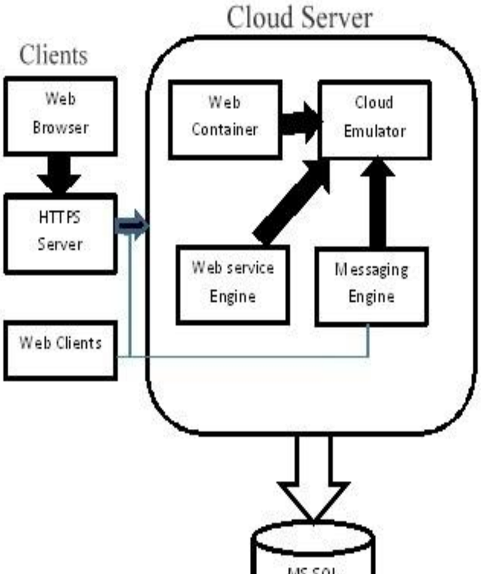

Fig. 6. Architecture diagram for proposed system.

The multi authority encryption will run the attribute key generation algorithm, and return the result to the user. For each Attribute Authority (AA), a user must have received from each user policy it allows to decrypt a data with set of attributes [3]. The main challenge in MA-ABE is to guarantee that two colluding users cannot each obtain keys from a different authority, and then pool their keys to decrypt a message that they are not entitled to.

E. ADVANTAGES OF PROPOSED SYSTEM

- Quickly find out the information about the patient heath record.
- In case of emergency doctor and other emergency department quickly get all the details all the informative details and start treatment.
- If in any condition doctors and medical facilities are not available the PHR owner itself able to take care of his health.
- On demand user revocation can be achieved.
- Key management issues can be solved.
- To provide data confidentiality and set access privileges can be achieved.

VI. CONCLUSION

The Personal Health Record system needs high level security against third party server. The PHR information is highly securedfunction for using Multi Authority-Attribute Based Encryption (MA-ABE). It plays aprominent role because these data are unique. Soit can’t be easily access by third party server. The ABE method addresses the unique challenges in multiple owner scenarios, in that we significantly reduce the Key complexity. So we adopt a novel based MA-ABE to encrypt PHR information in cloud computing. The major issues in existing method are key complexity, security, On Demand revocation etc. The proposed scheme overcome the major issuesby using the MA-ABE file encryption and also increasesthe securityfor sharing data in cloud system.

REFERENCES

[1] Attrapadung. A and Imai. H, “Conjunctive Broadcast and Attribute-Based Encryption”, Proc. Third Int’l Conf. Palo Alto on Pairing-Based Cryptography-Pairing, pp. 248-265, 2009. Yu. S, Wang. C, K. Ren, and W. Lou, “Achieving Secure, Scalable and Fine-Grained Data Access Control in Cloud Computing, ” Proc. IEEE INFOCOM ’10, 2010.

[2] Boneh. D, Gentry. C., and Waters. B, “Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys”, in Proceedings of the 25th Annual International Cryptology Conference, USA, pp. 258-275, 2005.

[3] Chase Melissa. ”Multi-Authority Attribute Based Encryption”. In TCC, volume 4392 of LNCS, pages 515–534. Springer, 2007.

[4] David Chernicoff, “HP VDI Moves to Center Stage, ” ZDNet, August 19, 2011.

[5] Goyal. V, Pandey. V, Sahai. V, and Waters. B, “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.

[6] Hur. J and Noh. D. K, “Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems”, IEEE Trans. Parallel an distributed Systems, vol. 22, no. 7, pp. 1214-1221, July2011.

[7] Li. M, 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, ” Proc. Sixth Int’lICST Conf. Security and Privacy in Comm. Networks (SecureComm ’10), pp. 89-106, Sept. 2010

[8] Li. Ming, Shucheng Yu, Yao Zheng, KuiRen, and Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption”, IEEE transactions on parallel and distributed systems, vol. 24, no. 1, january 2013.

[9] Liang. X, Lu. R, Lin. X, and Shen. X. S, “Cipher text Policy Attribute Based Encryption with Efficient Revocation”, technical report, Univ. of Waterloo, 2010.

[10] Mi. L, Lou. M, Ren. K, “Data security and privacy in wireless body area networks”, IEEE Wireless Communications Magazine (February2010).

[11] McDaniel. P, Pirretti. M, Traynor. P, and Waters. B, “Secure Attribute-Based Systems, ” J. Computer Security, vol. 18, no. 5, pp. 799-837, 2010

[12] Shanti. A. V. K and Vivek. G “A survey on fine grained access in cloud computing” International journal of applied engineering research ISSN0973-4562 Volume 9, number 21 (2014). PP. 10439-10444.

[13] Sun. Jin, Hu. Yupu, and Zhang. Leyou, “A Key-Policy Attribute-Based Broadcast Encryption”, The International Arab Journal of information Technology, Vol. 10, No. 5, September 2013

[14] Yu. S, Wang. C, Ren. K and Lou. W, “Achieving Secure, Scalable and Fine-Grained Data Access Control in Cloud Computing, ” Proc. IEEE INFOCOM ’10, 2010.

[15] Yu. S, Wang. C, Ren. K and Lou. W, “Attribute Based Data Sharing with Attribute Revocation, ” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS ’10), 2010.

[16] Zhang. L, Hu. Yu, and Mu. N., “Identity-Based Broadcast Encryption Protocol for Ad-hoc Networks”, in Proceedings of the 9th International Conference for Young Computer Scientists, Hunan, pp. 1619-1623, 2009.