ISSN:0975-9646

Using Advanced Encryption Standard for Secure and Scalable Sharing of Personal Health Records in Cloud

B. Sri Varsha[1], P.S. Suryateja[2]

[1]*M.Tech Student, Department of Computer Science and Engineering,*
Vishnu Institute of Technology
[2]*Assistant Professor, Department of Computer Science and Engineering,*
Vishnu Institute of Technology

***Abstract*— Cloud computing facilitates efficient management of Personal Health records. When the health records are uploaded on the cloud there is an advantage of easy accessibility. At the same time there is the risk of privacy and security. The data has to be encrypted and the patient should be able to control the data access. The managing of the Personal Health Records should be both scalable and secure. This paper addresses the issue of scalability and security. It proposes to use the concept of attributes for maintaining the data and corresponding keys are given to the users. This data is encrypted with Advanced Encryption Standard and then uploaded on the cloud.**

***Keywords*— Personal Health Records, Advanced Encryption Standard.**

I. Introduction

Cloud Computing has emerged as a superior platform for storing, managing and accessing data. Personal Health Records are being stored on clouds for efficient usage. On one hand there is an opportunity for efficient management of data and on the other there is the problem of privacy and security. A patient should have control over his health records. For privacy the data has to be encrypted properly. The patient should also have the privilege to grant access to persons only who have the corresponding key. This paper proposes to discuss how PHRs can be made scalable and secure.

II. Problem Definition

In a multiple owner and multiple user scenario the privacy of data and its accessibility are very crucial. The data should be encrypted before being placed on the cloud. The owner has to control data access. This being a complex phenomenon, the data access control should be simplified leading to simple key management.

III. Related work

Substantial work has been done in this aspect of making the data scalable and secure while making it patient centric. Attribute based encryption was proposed [1] for encryption as well as efficient key management. The concept is that the data will be encrypted under a set of attributes which enables multiple users to decrypt using the assigned key. The owner can encrypt the data without even knowing the Access Control List. The unique feature of ABE is that it prevents user collusion. Narayan etal [2] and Bethencort etal [3] proposed CPABE.

Patient Controlled encryption was suggested [4] which ensured privacy of the electronic health records. The patient selectively shares records among doctors and health care providers. The record of the patent is partitioned into a hierarchal structure and each part or portion is encrypted with its own matching key. The patient will have the main key and the remaining keys are distributed for decryption of the corresponding parts of the record.

Ming Lee etal [5] focus on the problem of private keyword searches on encrypted health records. Here users get the query capabilities from localized trusted authorities. They assure document privacy and query privacy.

IV. Proposed Framework

In this system the patient or the health care provider can upload and manage the data. The data of the patient's health records is maintained in such a way that the data is arranged based on attributes. The patient will have the privilege to delegate partial access rights to family, friends or designated health care providers. The files are uploaded and stored on the servers. The patient gives the different users the corresponding decryption key. Using the key the users will be able to access the relevant data only. The encryption and decryption process will be done using Advanced Encryption Standard. AES is employed as the chief encryption primitive. It is an encryption technique which uses the substitution and permutation method. The encryption is done in specified number of rounds. This makes the data secure.

V. Working of Proposed Frame Work

The key idea is, initially, through the admin process hospital registration is done only after getting license for that particular hospital. Then the doctors will get registered and patients also get registered. The patients can also claim for the insurance if they need. The patients' general information profile can be seen only by doctors who are having the Patient ID. The Patient ID can be shared to others by the patients (PHR owners). The patients can also share their information with others by uploading to the cloud.

A patient's health record comprises different types of data related to various areas like dentistry, cardiology, oncology, etc. The data in each area can also be of different types like lab reports, medical treatment, discharge summary and so on. Each of these files is based on a particular attribute. The owner will upload these files using Advanced Encryption Standard. A patient may want to share specific data with his doctor and may not want others to see the information. Therefore based on the attributes the owner will grant access to only that part of the record to those persons only with whom he wishes to share the data.

Additionally, in this framework, the data in the database is also encrypted. So that even if the intruders get access to database, they cannot read the data in the database. The data can be read only by the authorized persons in the framework like PHR owners, doctors. In this proposed system, donors such as blood donors can also register. All these details of the donors are accessed only by doctors. So, whenever the blood is required they can send message to the donors for the blood based on the blood group.

VI. System Architecture

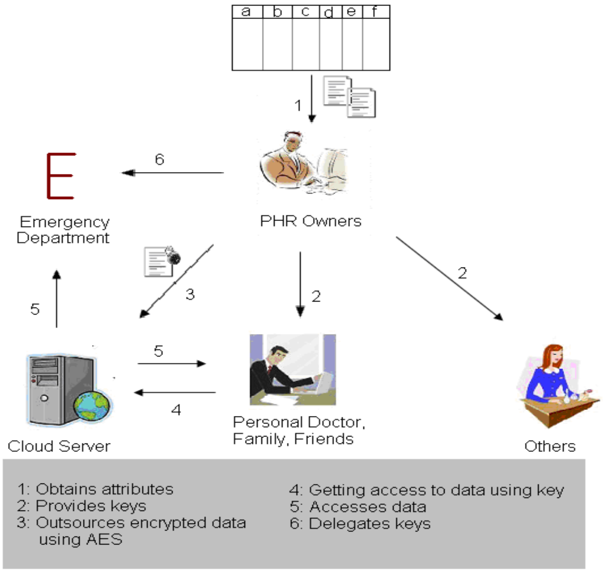

Fig. 1 Architecture

In Fig. 1,

(1) Initially the PHR owner selects the attributes to give the access rights to the users.

(2) The owner provides access keys to the users.

(3) Then, the PHR file is encrypted symmetrically with advanced encryption standard (AES) and the data owner stores the encrypted data on the trusted third party (cloud server).

(4) The users request the data from the cloud server using the access keys.

(5) The users can access the data from the cloud server after all the key verifications are completed and satisfied. The emergency staff in emergency department can also access the data using the keys in emergency situations.

(6) Here PHR owners assign the access keys to the emergency department for future purpose.

(7)

VII. Security

A. Security Issues

Data uploaded in the cloud can be tampered and modified. By using AES the privacy of the data is assured. In AES algorithm there are three different key sizes. Based on the key size the number of rounds is determined. This process is used to both encrypt and decrypt data. AES is used for secure transmission of data in the encrypted format.

B. Solutions

Data can be encrypted using several cryptographic algorithms. These algorithms may be symmetric or asymmetric. DES and AES are symmetric whereas RSA, ECC are asymmetric. The following table shows the performance of these algorithms.

Table I
Comparison between Symmetric and Asymmetric Algorithms

	DES	AES	RSA	ECC
Factors Contributor	IBM 75	Rijman, Joan	Rivest, Shamir 78	Neal Koblitz,Victor S. Miller
Key Length	56-bits	128,192, and 256	Based on No.of bit in N=p*q	135 bits
Block Size	64-bits	128 bits	Variant	Variant
Security Rate	Not enough	Excellent	Good	Less
Execution Time	Slow	More fast	Slowest	Faster

Among these AES is a strong algorithm.

C. Advanced Encryption Standard (AES)

1) To secure sensitive data, the United States has adopted the Advanced Encryption Encryption Standard (AES) as a standard algorithm to encrypt and decrypt sensitive information. AES is a symmetric block cipher which accepts a block size of 128 bits. It provides a choice of three different key lengths which can be 128 bits, 192 bits, or 256 bits; referred to as AES-128, AES-192, and AES-256 respectively. Based on the key length the number of rounds in the encryption process is determined, for instance, the number of rounds

- for AES-128 is 10,
- for AES-192 it is 12, and
- for AES-256 it is 14.

2) The major loop of AES executes the functions given below:

Functions of Advanced Encryption Standard
- SubBytes()
- ShiftRows()
- MixColumns()
- AddRoundKey()

AES makes use of 10, 12 and 14 rounds. After repeated transformation rounds, the plain text is converted into cipher text. This makes the data secure on the cloud.

3) *Implementation:* AES-128, AES-192, AES-256 (128, 192 and 256 are bits) process the data block in 10, 12, or 14 rounds respectively. The transformations are predefined. All the rounds are similar except the last one where there is no mix-columns. The rounds operate on two 128 bits i.e., state and round key. Each round from 1 to 10 or 12 or 14 uses a different round key.

The data block is processed as follows:

- The AES encryption routine starts by copying the 16-byte input array into a 4×4 byte matrix named State.
- Input data block also known as state is XORed with the first 128-bits of the cipher key.
- Then the resulting State is serially passed through 10/12/14 rounds.
- The result of the last round is encrypted data. The process of AES encryption algorithm using 128-bit key, is diagrammatically represented in figure 2.

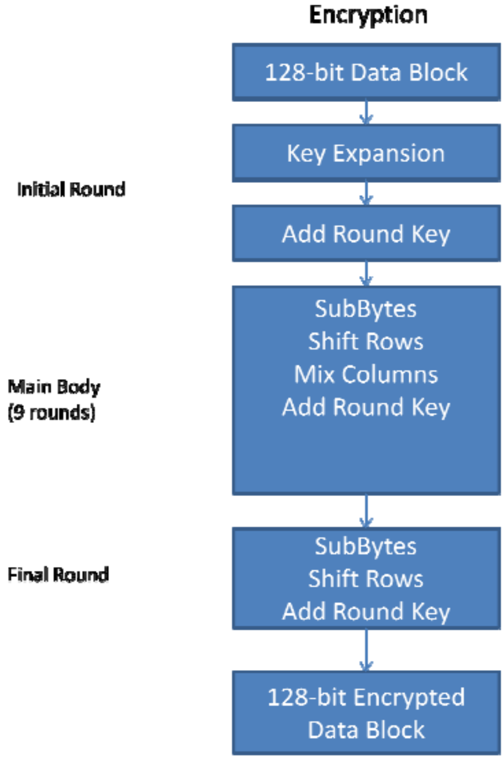

Fig. 2. Process of AES

4) *Algorithm:*

- Key Expansion: First from the cipher key the round keys are derived using the key schedule of Advanced Encryption Standard.
- Initial Round - AddRoundKey: Then each byte of the state is combined with the round key using bitwise XOR.
- Rounds
  - i) SubBytes: This is a non-linear substitution step where each byte is swapped with another according to a lookup table.
  - ii) ShiftRows: In this transposition step each row of the state is shifted cyclically in a certain number of steps.
  - iii) MixColumns*:* A mixing operation operates on the columns of the state, combining the four bytes in each column.
  - *iv)* AddRoundKey
- Final Round (no Mix Columns)
  - v) SubBytes
  - vi) ShiftRows
  - vii) AddRoundKey

5) In encryption AES is considered to be very suitable as it is less expensive when compared to ABE. Generally symmetric key is used for encrypting bulk of the data and asymmetric key like ABE is suitable for encrypting short key value. Here the data is encrypted using AES with any of the three types of keys— 128 or 192 or 256 bits key.

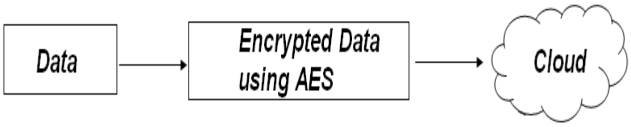

Fig. 3. Encrypting data with AES

Thus the PHR file is first encrypted symmetrically using AES algorithm key. Then the encrypted data is stored on the cloud server.

Using the assigned keys provided by the owner, the users can access the data.

VIII. Conclusion

The paper discusses the two crucial aspects of Personal Health Record management, those of security and data access control. Here the data is arranged attribute wise thereby facilitating access control and encrypted with AES which makes the record secure.

References

[1] Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data *ACM CCS (2006)*

[2] S. Narayan, M. Gagne´, and R. Safavi-Naini, "*Privacy Preserving EHR System Using Attribute-Based Infrastructure*," Proc. ACM Cloud Computing Security Workshop (CCSW '10), pp. 47-52, 2010.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption", Proc. IEEE Symp. Security and Privacy (SP ‟07), pp. 321-334,.

[4] Josh Benaloh, Melissa Chase, Eric Horvitz, and Kristin Lauter. Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records. research.microsoft.com.

[5] Ming Li∗ , Shucheng Yu† , Ning Cao∗ and Wenjing Lou. Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing. http://ualr.edu/sxyu1