Efficient and Secure Sharing of Personal Health Records Using Attribute-Based Encryption in Cloud Computing

V.Prathiba
Dept of Computer Science and Engineering,
Ratnavel Subramaniam College of Engineering,
Dindigul-624005

M.Vinoth Kumar M.Tech.
Assistant Professor,
Dept of Computer Science and Engineering,
Ratnavel Subramaniam College of Engineering,
Dindigul-624005

P.Anand Prabu
Dept of Computer Science and Engineering,
RVS College of Engineering and Technology,
Coimbatore-641014

Abstract— Recently, personal health record (PHR) has emerged as a patient-centric model of health information exchange, which features storing PHRs electronically in one centralized place, such as a third-party cloud service provider. Personal Health Record is web based application that allows users to directly enter their information such as diagnosis, medications, laboratory tests, immunizations and other data associated with their health. The intention of a PHR is to provide a complete and accurate summary of an individual's medical history which is accessible online. To ensure patients control over their own privacy, data encryption has been proposed as a promising solution. To achieve security of personal health records we use the attribute based encryption to encrypt the data before outsourcing it. Here we focus on multiple types of PHR owner scenario and division of personal health records users into multiple security domains which reduce key management complexity for owners and users. A high degree of patient's privacy is guaranteed.Extensive security and performance analysis shows that the proposed scheme is highly efficient. Our 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.

Index Terms—Personal health records, cloud computing, data privacy, attribute-based encryption

I. INTRODUCTION

Personal Health Record (PHR) concept has emerged in recent years. We can say that it is a patient centric model as overall control of patient's data is with patient. He can create, delete, modify and share his PHR through the web. Due to the high cost of building and maintaining data centers, third-party service providers provide PHR service. But while using third party service providers there are many security and privacy risks for PHR. As a matter of fact, PHRs are usually untethered, i.e.,provided by a third-party service provider, in contrast to electronic medical records (EMRs) which are usually tethered,i.e., kept by each patient's own healthcare provider. Untethered PHRs are the best ways to empower patients to manage their health and wellbeing.Web-based PHR solutions are essentially the same as electronic device PHR solutions, however, web-based solutions have the advantage of being easily integrated with other services.For example, some solutions allow for import of medical data from external sources.Solutions including RxVault.in, HealthVault, PatientsLikeMe, getHealtZ, onpatient, and

Careplan allow for data to be shared with other applications or specific people. 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 trusted. To ensure patient-centric privacy control over their own PHRs, it is essential to provide data access control mechanisms. Our approach is to encrypt the data before outsourcing. PHR owner will decide which users will get access to which data in his PHR record. A PHR file should available to only those users who are given corresponding decryption key. And the patient shall retain the right to revoke the access privileges whenever they feel it is necessary. The authorized users may either need to access the PHR for personal use or professional purposes. We divide types of users into two domains, personal domain and public domain. To protect personal health data stored on semi-trusted servers, we adopt attribute-based encryption as main encryption primitive. Using ABE, access policies are expressed based on attributes of users or data.

Scalability: „N‟ number of user can add into this application.

Security: For security purpose we are using Attribute Based Encryption (AES) and Message Digest5 (MD5) algorithm. We are encrypted data using AES algorithm and we are encrypted password using MD5 algorithm.

II. RELATED WORK

Key-Policy Attribute-based Encryption (KP-ABE): KP-ABE is a crypto system for fine grained sharing of encrypted data. In KP-ABE cipher text are label with attributes and private key are associated with access structures that control which cipher text a user is able to decrypt. It is used for securing sensitive information stored by third parties on the internet.

Cipher text Policy Attribute based Encryption (CP-ABE): CP-ABE is a policy to acquire complex control on encrypted data. This technique is used to keep encrypted data confidential [9].

Multi- Authority Attribute-Based Encryption (MA-ABE): MA-ABE method allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encryptor can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k [10].

III. PROPOSED SYSTEM

Personal Health Record is an internet based application that allows people to access and co-ordinate their lifelong health information and make if appropriate parts of its available to those who need. Personal Health Record‟s security and protection of its data have been of great concern and a subject of research over the years. There are many different forms of cryptographic mechanisms like AES, MD5 proposed to guarantee data security. In this work we propose a unique authentication and encryption technique using AES algorithm. In PHR data refers to the information that is collected, analyzed and stored. Example Medical history, List of medical problems, Medication history. The PHR owner herself should decide how to encrypt her file and to allow which set of users to obtain access to each file. In PHR infrastructure is the computing platform which processes or exchanges healthcare data such as software package and website.

Cloud Server: The main function of cloud server is to create interface between application and user. The authentication of the username and password is carried out. If user is authentic then he get access to his record.

IV. ATTRIBUTE BASED ENCRYPTION

Using attribute based encryption technique we are providing security to the database. A sensitive data is shared and stored on cloud server, there will be a need to encrypt data stored at third party. In Attribute based encryption cipher text labeled with set of attribute. Private key associated with access structure that control which cipher text a user is able to decrypt. We are using attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of the users. The complexities per

encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-retrieval to solve, and remain largely open up-to-date.

V. SYSTEM FLOW DIAGRAM

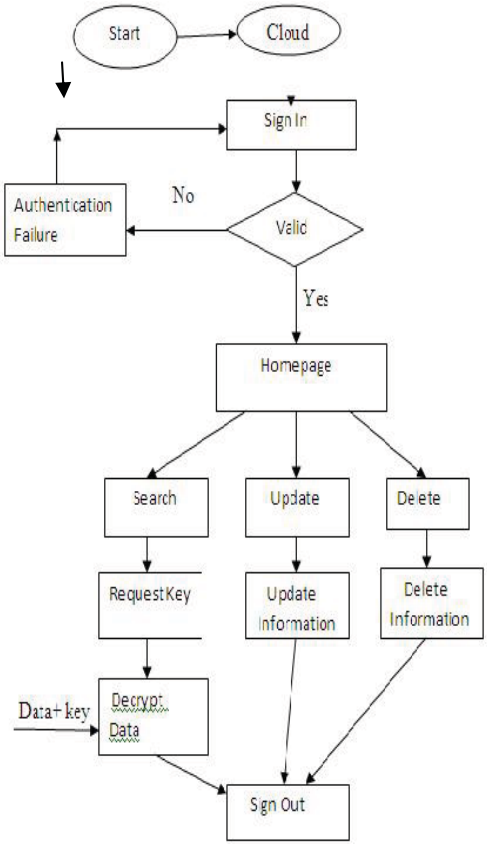

Fig 1. System Flow Diagram

VI. SYSTEM ARCHITECTURUL DIAGRAM

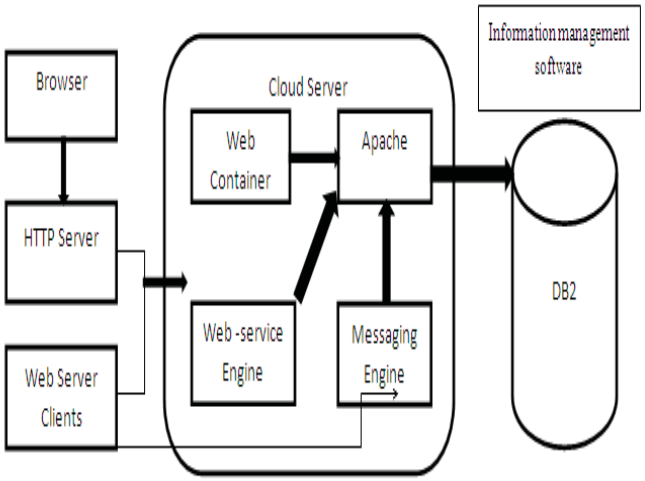

Fig 3. System Architecture

A. THE ATTRIBUTE HIERARCHY

We are using attribute based encryption for providing security. For that we use following distribution of attributes that are mainly important.

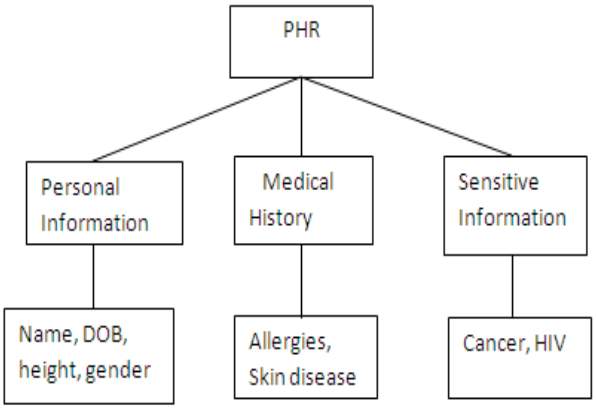

Fig 4. The attribute

B.AES

AES is an Advanced Encryption Standard used for secure transmission of data that is personal health record in encrypted format. In our system AES is used for sending user authentication data in encrypted format.

AES allows for three different key lengths:
128, 192, or 256 bits.

For encryption, each round consist of the following four step:

1) Substitute bytes
2) Shift rows
3) Mix columns

4) Add round key
The last step consists of XORing the output of the previous three steps.
For decryption, each round consists of the following four steps:
1) Inverse shift rows
2) Inverse substitute bytes
3) Add round key
4) Inverse mix columns. The third step consists of XORing the output of the previous two steps.
Step1: Substitute bytes

- This step consists of using a 16 × 16 lookup table to find a replacement byte for a given byte in the input state array.
- The entries in the lookup table are created by using the notions of multiplicative inverses in GF(28) and bit scrambling to destroy the bit-level correlations inside each byte.

Step2: Shift rows

- The first row of state is *not* altered.
- The second row is shifted 1 bytes to the left in a circular manner.
- The third row is shifted 2 bytes to the left in a circular manner.
- The fourth row is shifted 3 bytes to the left in a circular manner.

Step3: Mix columns

- Mix Columns for mixing up of the bytes in each column separately during the forward process. (The corresponding transformation during decryption is denoted Inverse Mix Columns and stands for inverse mix column transformation.)

- This step replaces each byte of a column by a function of all the bytes in the same column.

Step4: Add round key

- Add Round Key for adding the round key to the output of the previous step during the forward process. (The corresponding step during decryption is denoted Inverse Add Round- Key for inverse add round key transformation.)
- In this stage, the 128 bits of states are bitwise XORed with the 128 bits of the round key.
- The operation is viewed as column wise operation between is 4 bytes of state column and one word of the round key.

Advantages of AES:
1) AES is advanced method for secure and also it is powerful.
2) It provides the key length of 256 bits.

C.MD5

MD5 is cryptographic hash function in which produces 128bit hash value. The message digest algorithm is intended for digital signature application, where a large file must be “compressed”. For securing the password we are using MD5 algorithm. MD5 algorithm is one way encryption technique. Five step to compute message:
Step1: Append padding bits: Message is pad so its length is 448 mod 512.

Step2: Append Length Append a 64-bit length value to message Generate a message with 512 bits in length.

Step3: Initialize MD buffer Initialize a 4-word (128-bit) MD buffer (A, B, C, D) Word A: 01 23 45 67 Word B: 89 AB CD EF Word C: FE DC BA 98 Word D: 76 54 32 10

Step4: Process Message in 16-word block Process message in 16-word (512-bit) blocks.
Step5: Output.

VII. ADVANTAGES OF PROPOSED SYSTEM

1. Quickly find out information of patient details.
2. In case of emergency doctor and other emergency department quickly get all the details all the informative details and start treatment.
3. If in any condition doctors and medical facilities are not available the PHR owner itself able to take care of his health.
4. To provide easy and faster access information. 5.To provide user friendly environment.
6. To provide data confidentiality and write access control.

VIII. APPLICATION

Any organization can use this application to store their employees medical information.

IX. CONCLUSION AND FUTURE WORK

The personal health record system needs 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 hackable. In future we propose document privacy and query privacy to increase the efficiency and also we are reducing key management problem for enhancing 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 International Health Informatics Symposium, ser. IHI ˝10, 2010, pp. 220–229.

[3] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *CCS '09*, 2009, pp.121–130.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASSIACCS˝10, 2010.

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

[6] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS ˝08, 2008, pp.417–426.

[7] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. PrePrints, 2010.

[8] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.

[9] J. Bethencourt, A. Sahai, and B. Waters,"Ciphertext-policy attribute-based encryption," in *IEEE S& P '07*, 2007, pp. 321–334.

[10] Melissa Chase "Multi-authority Attribute based Encryption," Computer Science Department Brown University Providence, RI 02912.