International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A High Degree of Patient Privacy in PHR Patient-Centric Model of Health Information Exchange Using Cloud Security Technique

Rasal Swati A.[1], Pawar B. V.[2]

[1]M. E.(Computer Engg.) II Student, Padmabhushan Vasantdada Patil College of Engineering, Pune University, Pune

[2]Professor, Padmabhushan Vasantdada Patil College of Engineering,Pune University, Pune

Abstract: ***Personal health record (PHR) 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. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. Attribute-based encryption (ABE) is a promising cryptographic approach that achieves a fine-grained data access control. It provides a way of defining access policies based on different attributes of the requester, environment, or the data object. Especially, cipher text- policy attribute-based encryption (CP-ABE) enables an encryption to define the attribute set over a universe of attributes that a decryption needs to possess in order to decrypt the cipher text, and enforce it on the contents. Thus, each user with a different set of attributes is allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the data storage server for preventing unauthorized data access, which is the traditional access control approach of such as the reference monitor. A high degree of patient privacy is guaranteed simultaneously by exploiting multi authority ABE. This scheme 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 proposed scheme.***

Keywords: Personal health records, cloud computing, data privacy, fine-grained access control, attribute-based encryption

1. Introduction

Cloud Computing is internet based service which provides different type of services like applications, resources on demand basis. Cloud Computing is sharing of resources on a larger scale which is cost effective and location independent. Resources on the cloud can be deployed by the vendor and used by the client. The most important is that the customers do not need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money. Cloud is sold on demand, typically by the minute or the hour; it is elastic a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). A cloud can be private or public. A public cloud sells services to anyone on the Internet. A private cloud is a data center that supplies hosted services to a limited number of people. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services. From last few years cloud computing is more popular, but it has some security problems, when it comes to Security, cloud really suffers a lot. The vendor for Cloud must make sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by masquerade a legitimate user, there by infecting the entire cloud thus affecting many customers who are sharing the infected cloud. Some of the problem which is faced by the Cloud computing, like data integrity, data theft, privacy issues, infected application, data loss, data location etc. When a data is on a cloud anyone from any location can access those data from the cloud. Cloud does not differentiate between a sensitive data from a common data thus enabling anyone to access those sensitive data. Thus there is lack of data integrity in cloud computing.

2. Related Work

A patient usually goes to hospital which is near by their home for routine check-up or health services and their health information is stored in their local database. Sometimes the patient need to go another healthcare center due to several reason like unavailability of service on holidays, need for specialized health centres. The health information stored in the health care centers is only accessible to the employees of that Center and hence flow of information gets limited. So instead of storing information on local database we can store this information in third party i.e. cloud service provider [1].By the literature survey, following issues are identified:

- Security
- Key complexity
- User Revocation

Our ultimate objective is to provide solution to the identified issues. Our proposed system will solve security and key management problem by making use of homomorphic encryption [1]. The key idea is to divide the system into multiple security domains (namely, public domains and

personal domains) according to the different user's data access requirements. Some other issues in data outsourcing situation are the implementation of authorization policies and the policy updates. There are several challenges regarding attribute and user revocation[5]. We are focusing on multiple data owner scenario and it will supports an efficient on-demand User/attribute revocation and provide emergency access through break glass.

3. Proposed Work and Framework

The novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs they use attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. In secure data outsourcing, they focus on the multiple data owner scenario and a high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE. It enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios [1].

The confidentiality of personal health records is a major problem when patients use commercial Web-based systems to store their health data. Traditional access control mechanisms have several limitations with respect to enforcing access control policies and ensuring data confidentiality. In particular, the data has to be stored on a central server locked by the access control mechanism, and the data owner loses control on the data from the moment when the data is sent to the server. In CP-ABE, the data is encrypted according to an access policy over a set of attributes. The access policy specifies which attributes a user needs to have in order to decrypt the encrypted data. Once the data is encrypted, it can be safely stored in an untrusted server such that everyone can download the encrypted data but only authorized users who satisfy the Access policy can decrypt [2].

3.1 Scope

Our proposed system will have following features:

- Cloud Computing provides different type of internet based services like secure access of Personal Health Record, PHR is an emerging patient centric model which is used for exchanging and storing of health information and this information is stored at third party, such as cloud providers.
- In proposed system we will try to minimize issues regarding privacy exposure, complexity in key management by providing role based access policy for personal health record using Homomorphic cryptosystem.
- Our system will work on key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. The owners directly assign access privileges for personal users and encrypt a PHR file.
- A Homomorphic Encryption is the conversion of data into cipher text that can be analyzed and worked with as if it were still in its original form. Homomorphic Encryption are used to perform operations on encrypted data without knowing the private key (without decryption).

3.2 Methodology

3.2.1 System Architecture

As shown in figure 1, any user can create personal health record and store it on cloud server such user is known as PHR owner.PHR owner has full control on his/her record. He/She can create, manage and control record. To obtain secure data sharing and access control to PHRs which is stored in cloud servers are fully controlled by the patient. A high degree of patient privacy is ensured by using Homomorphic Encryption technique and store this PHR in encrypted format. Anyone can download encrypted PHR but the user who provides corresponding decryption key can access the record.

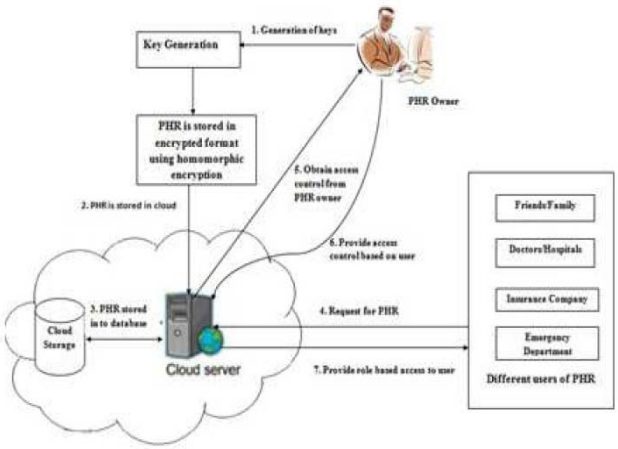

Figure 1: System Architecture

For secure data storage, the users are divided in the PHR system into multiple security domains that greatly reduces the key management for owners and users. In this we propose mechanism for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. Each PHR owner access is given to the emergency department i.e. ED. If any emergency situation is occur then emergency staff needs to communicate with ED for accessing PHR record and verify its identity and emergency situation, and obtain temporary read key to access his/her PHR. To achieve secure and scalable role based access for personal health record we can use homomorphic encryption. With the use of homomorphic encryption cloud can perform functional computation on encrypted data and send this patient updates, alerts based on the received data. Our proposed work can be divided into following modules:

1. Key Generation Module
2. Encryption and Decryption Module
3. Role-based access policy Module
4. Analysis Module

3.2.2 Key Generation Module

By using Elgamal homomorphic encryption algorithm we will generate two keys i.e. private key privk and public key pubk. Figure 2 shows the process of key generation. Key generation has to initialize key length and algorithm

parameter then it will calculate Genkeypair () to key pair. It will produce key pair i.e. private key and public key.

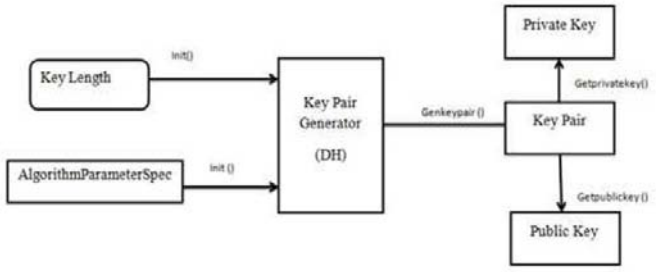

Figure 2: Key Generation Process

3.2.3 Encryption and Decryption Module

A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. In proposed system data is stored in encrypted format. Anyone can download encrypted PHR but only those user can read data who provides corresponding decryption key. Algorithm for encryption:

1. Obtain the public key.
2. Prepare M for encoding: Write M as set of integers (m1, m2.....)in the range of (f1, ..., p-1). These integers will be encoded one by one.
3. Select random exponent: In this step, PHR owner will select a random exponent k that takes the place of the second party private exponent in the Diffe-Hellman key exchange.
4. Compute public key.
5. Encrypt the plaintext.

$$c_i = m_1 * (g^b)^k$$

Algorithm for decryption:
1. Compute shared key:
The ElGamal cryptosystem helped PHR owner to define a shared secret key without user interaction. This shared secret is the combination of user private exponent b and the random exponent k chosen by PHR owner. The shared key is defined by the following equation:

$$(g^k)^{p-1-b} = (g^k)^{-b} = b^{-bk}$$

2. Decryption: For each of the ciphertext parts ci Bob now computes the plaintext using following equation

$$m_i = (g^k)^{-b} * c_i \bmod p$$

4. Conclusion

In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. Through implementation and simulation, we show that our solution is both scalable and efficient.

References

[1] Ming Li, Member, IEEE, Shucheng Yu, "Scalable and secure sharing of personal health record in cloud computing using attribute based encryption [1]," IEEE TRANSACTIONSON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013.
[2] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," technical report, Univ. of Twente, 2009.
[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security, (ASIACCS 10),2010.
[4] M. Li, S. Yu, N. Cao, and W. Lou , "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Intl Conf. Distributed Computing Systems (ICDCS 11), June 2011.
[5] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation[5]," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008