Secure and Role-Based Access Policy for PHR using Homomorphic Cryptosystem

Swapna H. Dhokate[1], Gauri J. Sutar[2], Pranali S. Kambale[3] , Karima M. Shaikh[4]
[1]B.E(CSE)Student, Daulatrao Aher College of Engineering, Maharashtra, India
[2]B.E(CSE)Student, Daulatrao Aher College of Engineering, Maharashtra, India
[3]B.E(CSE)Student, Daulatrao Aher College of Engineering, Maharashtra, India
[4]B.E(CSE)Student, Daulatrao Aher College of Engineering, Maharashtra, India

---***---

Abstract – *Cloud computing, is an emerging computing environment which allows user to remotely store data. The data can be stored in one centralized place. Without any installation of applications, users can use applications and access their personal files at any computer with internet access. Personal Health Record (PHR) is a Patient-Centric model for health information exchange. By using this, users can store their Personal Records on a trusted third party i.e. cloud providers. But, there are many challenges related to data security and access control. To overcome such problems Cryptographic methods were used. The data can be encrypted before outsourcing. Yet, there were issues of privacy exposure, scalability in key management and flexible access. In this paper, we propose a novel penitent centric framework and suite of mechanisms for data access control to the PHRs which are stored on semi-trusted servers. To achieve scalability in key management, flexible access and patient's privacy the Homomorphic Encryption*

Technique is used. Dynamic modifications in access policies, supports efficient on-demand user/attribute revocation and break glass access under the emergency scenario. For providing security, in PHR system the users are divided into different domains.

***Key Words*: Cloud Computing, Personal Health Record (PHR), Homomorphic Encryption Technique Data Confidentiality**

1. INTRODUCTION

1.1 Cloud Computing

Cloud Computing is a type of computing that relies on sharing pool of physical and/or virtual resources, rather than deploying local or personal hardware and software. The only thing that user must be able to run the cloud computing systems interface software, which can be as simple as Web Browser, and cloud network takes care of the rest. Cloud computing uses internet and central remote servers to maintain data and applications. This technology allows much more efficient computing by centralizing storage, processing and bandwidth. The biggest advantage of cloud computing is that, users can access stored data at any computer with internet access. The main benefit of cloud computing is flexibility.

1.2 Personal Health Record

Personal Health Record (PHR) is an emerging patient-centric model for health information storage and exchange. Building and maintaining specialized data canters requires higher cost, it causes the PHR services provided by the third party service providers like Microsoft Health Vault, Google Health. These service providers cannot be fully trusted, so the patient loses their control over PHRs when they store their records in cloud servers. Since the cloud computing is an open platform, the servers are subjected to malicious outside attacks [2]. PHR system allows user to create, manage, and control their Personal Health Records. PHR is an electronic record stored on a trusted third party server i.e. cloud server. It uses services provided by the cloud service providers. The cloud services are broadly divided into three categories: Iaas (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service). Cloud computing is a delivery of service rather than product, software or shared resources. In This PHR system, each patient has full control on his own records and can share his records with wide range of authorized users.

In existing system there were some issues regarding to patient's privacy, data access control, scalability in key management and flexible storage. To achieve data privacy issues, in this PHR system the Homomorphic encryption technique is used. To prevent unauthorized users from accessing information, a feasible and promising approach is data should be encrypted before being outsourced [1]. To avoid the key management complexity, the PHR system is divided into two different domains: one is Personal and second is the Public domain. The friends and family members should be included in the Personal domain while hospital, Health service providers are included in the public domain.

2. Overview of Framework

The main goal of our framework is to provide a novel patient-centric secure model for storing and exchanging the information. To design a PHR system where there are multiple PHR owners and Multiple PHR users. The PHR owner creates, manage, delete record and can store it in cloud server. He has full control of his PHRs and can share his records with a wide range of users. The users who want access of records are from various aspects like friend, family member, doctor, nurse or any other Health service provider. Users access PHR documents through the server

.The server is a semi-trusted server i.e. honest but curious that means server will follow protocol in general but simultaneously try to access files beyond privileges[3]. Hence from the security point of view the system is preloaded with public/private key pair. The objective of system is to achieve the data confidentiality by preventing unauthorized access to data. To restrict the write access control, it means only PHR owner can perform write on his records. To support on-demand revocation.

3. System Architecture

The proposed system is developed for securely storing and maintaining health records. The system has various components that are:

PHR Owner

PHR Users

Cloud server

Emergency staff access

1. PHR Owner

   PHR owner is a person who creates his personal health records in electronic form. He can also manage his records stored in cloud. PHR owner has full access control over his records, so he can share records with his friends, doctors, nurses to get clinical suggestions.

1. PHR User

   The PHR user may be from personal domain or from public domain. Users can have rights acceding to their roles. The users in personal domain include friends or family members while users in public domain include doctors, nurses, and insurance agents.

2. Cloud server

   Cloud servers is a storage area.PHR owners uses cloud servers for storing his data and maintaining PHRs. So, building and maintaining data centers is not needed. Cloud data storage services provide some benefits like availability, scalability, low cost and on-demand sharing of data among the authorized (trusted) users. The data owner has to verify that whether his data is being correctly stored and maintained in cloud or not. This third party (cloud servers) cannot be fully trusted, because of it's open nature malicious attacks may happens. In this proposed system, each and every data is stored in an encrypted format and without key no one can decrypt and get original data.

3. Emergency staff access

   The access rights of PHRs of each PHR owner are delegated to an Emergency Department(ED).The emergency staff needs to contact with the Emergency Department to verify his identity and the emergency situation.

4. Implementation Details

4.1. Methodologies

There are four modules in this framework:

1. User Registration with Role

2. Key Generation

3. File Upload and Encryption

4. Role Verification and File Download

1. User Registration with Role

The key idea is dividing the users into two domain that are personal and public domains. The user is registered to the PHR system with their role. The user may be PHR owner, individual user, hospital or any health organization. As per user's role they have file accesses. If the user is a PHR owner then he will have to fulfill all his personal info first and then he will be able to upload his files onto cloud. For privacy purpose the all the PHR's data and files are stored in an encrypted form.

2. Key Generation

   Each PHR owners client application generates a it's corresponding public or master key. The data owner specifies the access policies of data reader in his personal domain and generates a secret key. The users can get the secret key from data owner through the email.

3. File Upload and Encryption

In this module, the owner can be able to upload his health records which can be of any type. It may be text, pdf, doc file. The files must be encrypted before storing on cloud. Some Cryptographic algorithms are used here like TDES (Triple Data Encryption Standard), MD5 (Message Digest) Algorithm. The encrypted file can be decrypted on by the authorized users.

Homomorphic encryption plays an important role in cloud computing, allowing PHR owners to store encrypted PHR files in public cloud and take advantage of services provided by the cloud service providers. This technique prevents the rouge insiders from violating privacy. It also prevents the accidental leakage of personal sensitive information.

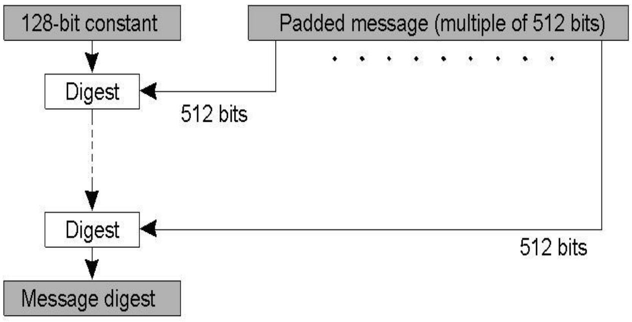
5. Role Verification and File Download

The users can send requests for accessing files through servers. When user requested any file, the role of user is verified. If user is authenticated, then only he will get rights to access a particular file of particular person. The authorized user will obtain a secret key, which can be used for decrypting and downloading the file. If the user entered secret key matches with the original secret key then only that user can decrypt the file.

4.2. Cryptographic Algorithms

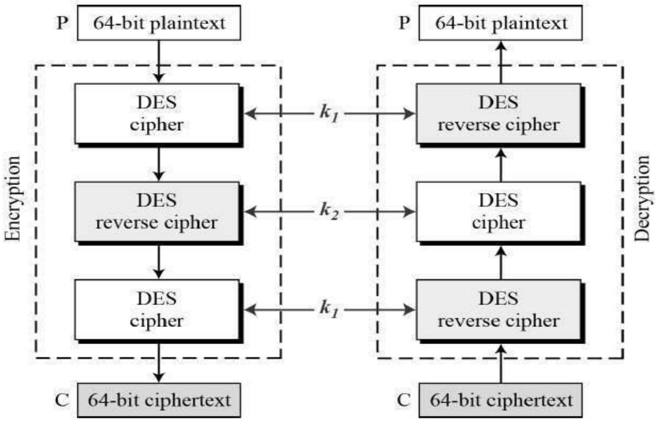
MD5 (Message Digest) Algorithm:

The MD5 algorithm takes input message of any length and produces output as 128-bit “fingerprint”, “message digest” or “hash”. It is conjectured that it is computationally infeasible to produce same hash or message digest for two messages. The hash value is unique to every file irrespective of it’s size and type.



TDES (Triple DES) Algorithm:

TDES is another mode of DES (Data Encryption Standard). The procedure for encryption is same as regular DES, but it is repeated three time; therefore it is named as Triple DES. Data is encrypted with first key, decrypted with second key and again encrypted with the third key. Same procedure is followed, but in reverse manner while decrypting data. There are three modes of TDES that are: ECB (Electronic Codebook), CBC (Cipher Block Chaining) and CFB (Cipher Feedback).



5. CONCLUSIONS

This framework allows users to store and maintain their health records in a secure and scalable way. Records stored on cloud in an encrypted form, so the privacy risk is reduced. Different cryptographic algorithms are used here for providing security to data. This paper demonstrates that, by using homomorphic cryptography PHR owners can stored their records securely on cloud server which is semi-trusted. The framework addresses and reduced the challenges regarding to key management brought by the multiple owners and multiple users.

REFERENCES

[1] ”Overview of Efficient and secure Personal Health Record storing in cloud computing”, IJISET, Volume 1, June 2014Soniya Patil and K. Nagi Reddy.

[2] “At Risk of Exposure-in the push for electronic medical records, concern is growing about how well privacy can be safeguarded,” 2006. [Online]. Available:http://articles.latimes.com/2006/jun/26/health/he-privacy26

[3] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, “Over-encryption: management of

access control evolution on outsourced data," in VLDB '07, 2007, pp. 123–13 R. Nicole,

[4] "Scalable and Secure Sharing of Personal Health Records in cloud Computing using Attribute-Based Encryption" Ming Li , Shucheng Yu, Yao Zheng Kui Ren, 2006

[5] "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner setting", M.Li, S.Yu, K.Ren and W.Lou, Sept 2010

[6] "Secure and efficient way of handling personal health records in cloud computing", Kalaiprasath. R, R.Udayakumar, R.Elankavi, May 2013