RESEARCH ARTICLE OPEN ACCESS

Hybrid Security and Fine-Grained Access Control for Personal Health Record in Cloud Computing

P.Naresh Kumar[1] P.Venkateswara Rao [2]
PG Student[1] M.Tech, Associate Professor[2]
Department of Computer Science and Engineering,
Audisankara College of Engineering & Technology, Gudur
A.P-India

ABSTRACT
Now a days, Personal Health Record become patient-centric model in which PHR service allows a patient to manage and control personal health data on one place through the web, which has made the storage, retrieval and sharing of the medical information more efficient. For the wide range access it has out sourced in third party storage such as cloud providers. These PHR contains sensitive data that should be protected from unauthorized parties. But while using third party service providers there are many security and privacy risks for PHR. the one way to protect PHR data is to encrypt data before out sourcing. Since the PHR has been accessed by the multiple authorities, we introduce a fine grained attribute based access control in which each party is assigned with access permission for a set of attributes. Division of personal health records users into multiple security domains which reduce key management complexity for owners and users.
Keywords:- Personal Health Records, Cloud Computing Hybrid cryptography, Symmetric Key Encryption, Asymmetric key Encryption

I. INTRODUCTION

Personal Health Record (PHR) became an emerging patient centric model for the exchange of personal health information through third party such as cloud Providers. Since it is being out sourced, the patients have no more physical control over the health Information. There are wide ranges of security and Privacy concerns while storing the data to the cloud. To ensure the security and privacy of the health record, the data should encrypt before outsource it. Yet, there are other issues toward achieving fine-grained, cryptographically enforced data access control are efficient key management, dynamic user revocation and flexible access.

This paper presents a different approach from the previous work for encrypting the information. The patient can decide with whom the information should be shared. For the fine-grained access of information, here introduces an architecture in which upon request from a person, a virtual proxy server will be created for the purpose of accessing the information. Only the person who has the decryption key can enter in to the virtual proxy server. This approach has made the user

Revocation process much easier since the key can be used only one time.

Scalability: Any number of users can added to the system using the proposed approach.

Security: Here for the encryption hybrid cryptography is used. Symmetric key cryptography is used for data encryption and Asymmetric key cryptography is used for key encryption.

Efficiency: Since it uses both Symmetric key and Asymmetric key cryptography it is fast and very secures.

CLOUD USE:
Cloud computing is very large storage to any type of data. Cloud computing is new technology and it is become very essential for industry.
Cloud computing comes into focus only when you thinks about, what IT always needs a way to increase capacity or add capabilities on the fly without investing in infrastructure, training new persons, or licensing new software.

II. CLOUD COMPUTING ARCHITECTURE

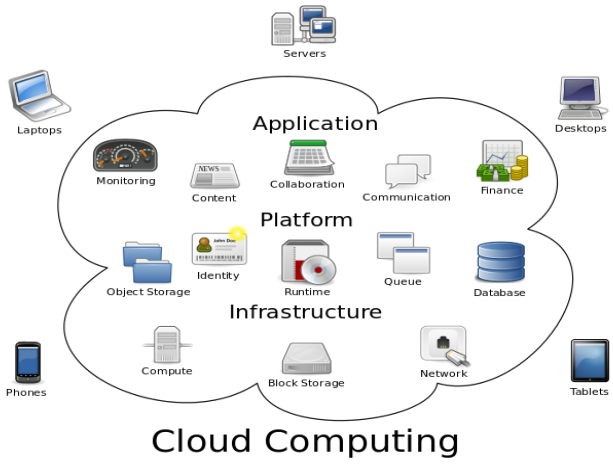

Figure 1: Cloud Computing

III. EXISTING SYSTEM

In the existing system either it uses Symmetric key encryption or it uses Asymmetric key encryption. Symmetric key encryption is simple and easy to carry out. Asymmetric key encryption is faster than any other cryptographic techniques.

Since it uses same key for both encryption and decryption, the keys should be exchanged between sender and receiver. Exchanging the key is a disadvantage, since it can be retrieved by a third party. It will leads to key escrow problem. Assign a central authority to keep the key will lead to trust that party completely. Collusion attack is a disadvantage of the existing system. Origin and authenticity of message cannot be guaranteed. Asymmetric key encryption is more secure than Symmetric key encryption since it uses different keys for encryption and decryption. But compared to symmetric key encryption, Asymmetric encryption is relatively slow and is not feasible for decrypting message. It uses more computational resources.

A Symmetric key Encryption

A single-key encryption system (also known as "Symmetric key encryption", since the same key is used for both encryption and decryption) works by means of an algorithm that transforms the input data based upon the value of an encryption key, using some combination of mathematical and logical operations. To decrypt, the algorithm runs the same set of operations in reverse, using the same key value.

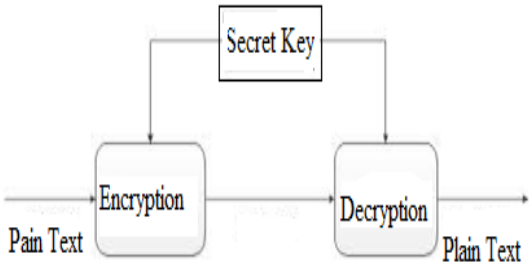

Figure 2: Symmetric key cryptographic

The Asymmetric key algorithms allow one key to be made public while retaining the private key in only one location. They are designed so that finding out the private key is extremely difficult, even if the corresponding public key is known. A user of public key technology can publish their public key, while keeping their private key secret, allowing anyone to send them an encrypted message.

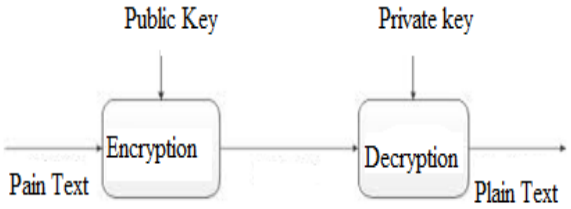

Figure 3: Asymmetric key cryptography

IV. PROPOSED SYSTEM

Personal Health Record is patients centric web application in which a patient can access manage and control their health information in a fine-grained manner. For the wide range of access these health records are outsourced to cloud servers. In recent years many research have been done on the security and privacy of these cloud servers. Most of the researches have been concluded with the fact that the data should be kept securely by encrypting the data before out sourcing it. In this proposed work, it uses a cryptography technique called Hybrid Cryptosystem that is different from the previous work.

A. Hybrid Cryptography

In cryptography, public-key cryptosystems are convenient in that they do not require the sender and receiver to share a common secret in order to communicate securely (among other useful properties). However, they often rely on complicated mathematical computations are thus generally much more inefficient than comparable Symmetric-key cryptosystems.

In many applications, the high cost of encrypting long messages in a public-key cryptosystem can be prohibitive. A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a Symmetric-key cryptosystem.

1) Methodology for cryptosystem

A hybrid cryptosystem can be constructed using any two separate cryptosystem:

1. A key encapsulation scheme, which is a public-key cryptosystem.
2. A data encapsulation scheme, which is a Symmetric-key cryptosystem.

The hybrid cryptosystem is itself a public-key system, who's public and private keys are the same as in the key encapsulation scheme. In place of public key system we can use digital signature like message digesting function with symmetric key system to make hybrid crypto system. Note that for very long messages the bulk of the work in encryption decryption is done by the more efficient symmetric-key scheme, while the inefficient public-key scheme is used only to encrypt / decrypt a short key value.

B. Block diagram for Hybrid Cryptosystem

The block diagram of proposed hybrid cryptosystem is shown in figure 4, plaintext encrypted by proposed Symmetric encryption algorithm to produce Cipher text, then message digesting function is also apply on plain text by using SHA-160 to produce message digest of plain text. Now again applying proposed encryption technique on produced message digest text so it will also convert in Cipher text now combine both Cipher values (c1 and c2) into one and send to the receiver.

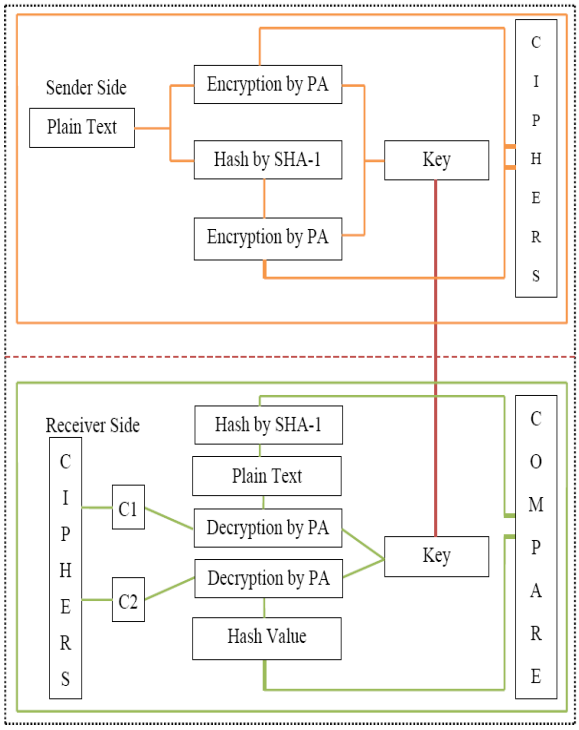

Figure 4: Hybrid cryptosystem

At receiver end, separate both Cipher (c1 and c2) values and apply proposed decryption algorithm one by one on each Cipher value. From first Cipher value plain text will get and from second Cipher value c2 message digest will get. Then apply message digesting function SHA-1 on plain text which is produced during decryption to produced message digest. Now finally comparing both message digests values with each other for changes in message digest. If both message digests are same then plain text securely received otherwise original plain text is tempered by the hacker so drop the whole information.

Basically this technique is a method of encryption that combines two or more cryptography technique and usually includes a combination of Symmetric and message digesting function to take benefit of the strengths of each type of technique. Symmetric encryption has the performance advantage and therefore is the common solution for encrypting and decrypting performance sensitive data, such as an online data stream. However, Symmetric encryption has a downside, i.e. cryptography key needs to be known to the both sender and receiver of encrypted data, and the exchanging of the key over an insecure channel may cause security risks. On the other hand, message digesting provides better security in that the message digesting provides digital signature and support to integrity principal.

Proposed research is the designing and implementation of a new Hybrid concept. Proposed technique is a method of encryption that combines two or more cryptography technique and usually includes a combination of Symmetric and message digesting technique to take benefit of the strengths of each type of cryptography.

Basically there are four security principles “Confidentiality”, “Integrity”, Authentication” , and “ Non-Repudiation” , in which Symmetric technique fulfil the concept of confidentiality, it also provide the performance advantage and therefore is the common solution for encrypting and decrypting performance sensitive data. On the other hand, message digests technique is fulfil the authentication as well as integrity security principle concept to provide better security in the cryptography.

C. Advantages of Proposed System

1. Health information can be accessed easily and quickly.
2. Treatment can be quickly started using the information recorded.
3. Patient can shown the details to other doctor for medical advice in a controlled manner.
4. Reimbursement procedure can be done easily.
5. A uses friendly environment is provided.
6. Data confidentiality.

V. RESULT

Cryptographic key needs to be known to both the sender and receiver of encrypted data, and the exchanging of the key over an in secure channel may cause security risks. On the other hand, message digesting provides better security in that the message digesting provides digital signature and support to integrity principal. Proposed research is the designing and implementation of a new Hybrid concept.

VI. CONCLUSION AND FUTURE ENHANCEMENT

This paper provides privacy and security to the medical data which is stored in the third party cloud storage. It prevents attackers and hackers by using new cryptographic techniques like hybrid encryption.

However, using hybrid encryption is more secure than any other techniques that are used till now, data needs more security. If the key that has to be encrypted is as same length as the message then, using public key cryptography is of no use. So a new technique should be introduced for the same. Now days there are many cryptographic present for the efficient encryption and decryption. These can be adopted for

the better security for the data's that are stored in the cloud storage.

ACKNOWLEDGEMENT

This work was supported by P. Venkateswara Rao, M.Tech, (PhD) Associate Professor, Deportment of Computer Science and Engineering through his valuable guidance, constant encouragement, constructive Criticism and keen interest.

REFERENCES

[1] U.jyothi k, Nagi Reddy, B.Ravi Prasad," Review of" Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" " international journal of engineering and computer science ISSN:2319-7242 Volume 2 issue 8 August, 2013 page no.2440-2447

[2] M. Li, S. Yu, N. Cao, and W. Lou, " Authorized private keyword Search over Encrypted personal Health Records in Cloud Computing," Proc 31stInt' l Conf. Distributed Computing System (ICDCS'11), June 2011.

[3] 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," Proc. Sixth Int' l ICST Conf. Security and Privacy in comm. Networks (Secure Comm.' 10), pp. 89-106, sept.2010.

[4] H. Lo" hr, A-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), PP.220-229,2010.\

[5] S. Yu, C. Wang, K Ren, and W. Lou, "Achieving secure, Scalable and Fine-grained Data Access Control in Cloud computing", prc. IEEE INFOCOM '10, 2010.

[6] C. Dong, G. Russell, and N. Dully, "Shared and Searchable Encrypted Data for Untrusted Servers," j. Computer Security, vol. 19, pp. 367-397, 2010.

[7] J. Benaloh, M. Chase, E. Horvitz, and K. lauter, "patient Controlled Encryption: Ensuring Privacy of Electronic medical Records", proc. ACM workshop Cloud computing security (CCSW '09), pp. 103-114, 2009.

[8] G. Ateniese, K Benson, and S. Hohenberger, "Key- Private Proxy Re-Encryption, "proc. Topics in Cryptology (CT-RSA), pp.279-294, 2009.

[9] J. Shao and Z. Cao, "CCA-secure proxy Re-Encryption without pairing. " Proc. 12th Int'l Conf. Practice and Theory in public Key Cryptography (PKC), pp. 357-376, 2009.

[10] Q. Tang, "Type-Based proxy Re-Encryption and its construction, "proc. Ninth Int'l Conf. Cryptology in India: progress in Cryptology (INDOCRYPT), PP. 130-144, 2008.