A Safety Key Management for Privacy and Preserving Data in Cloud

Rani.S, Dhivya D.T

Assistant Professor, Department of Information Technology
P.B College of Engineering, Chennai, Tamilnadu, India.
raniparthiban@gmail.com

Assistant Professor, Department of Information Technology
P.B College of Engineering, Chennai, Tamilnadu, India.
dt.dhivya@gmail.com

Abstract— **The Data in health care applications are digitalized in order to improve security**. **By combining several well-designed cryptographic mechanisms and developing a key management scheme to facilitate the interoperation among these mechanisms, the risk of illegal distribution can be reduced. Even authorized person may hack the data. Therefore, this paper provides a Split-Key encryption technology and homomorphic key encryption in cloud. The noteworthy term isn't encrypting the data– it's protecting the encryption keys. Every time an application accesses a data store, it needs to use the encryption keys. Virtual Key Management is the first solution to keep your cloud data truly secure.**

Keywords— **Cryptography, Encryption, Split-Key Encryption, Homomorphic Key Encryption Virtual Key Management.**

I. INTRODUCTION

Interest is increasing in the security of electronic medical information, or patient health information, that is digitally stored. Sometimes this information needs to be accessed for physicians to be able to make the best decisions about patient care. Patients have the right to determine how and when their health information is shared. Radiologic images, lab test results, medications, allergies, and other clinical information are increasingly being stored and viewed on computers. The responsibility that physicians have to protect their patients from harm extends to protecting patient information, privacy and confidentiality. Patient information security includes the steps healthcare providers must take to guard patients' "protected health information" commonly referred to as PHI, from unauthorized access or breaches of privacy or confidentiality. Security also refers to maintaining the integrity of electronic medical information, and ensuring availability to those who need access and are authorized to view such clinical data, including images, for the purposes of patient care.

Patient privacy refers to the right of patients to determine when, how and to what extent their health information is shared with others. It involves maintaining confidentiality and sharing identifying data, known as protected health information (PHI), only with healthcare providers and related professionals who need it in order to care for the patient.

Cloud computing [3] is clearly one of today's most enticing technology areas due to its cost-efficiency and flexibility. Cloud computing is Internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customers on a pay-as-you-use basis. All information that a digitized system has to offer is provided as a service in the cloud computing model. Users can access these services available on the "Internet cloud" without having any previous know-how on managing the resources involved. Thus, users can concentrate more on their core business processes rather than spending time and gaining knowledge on resources needed to manage their business processes.

Cloud computing customers do not own the physical infrastructure; rather they rent the usage from a third-party provider. This helps them to avoid huge. They consume resources as a service and pay only for resources that they use.

When it comes to protecting data in the cloud, the biggest challenge isn't encrypting the data– it's protecting the encryption keys. Every time an application accesses a data store, it needs to use the encryption keys. This puts them at risk in two places: when they are stored, and when they are in use. Virtual Key Management is the first solution to keep your cloud data truly secure. Virtual Private Data is the only system available that offers the convenience of cloud-based hosted key management without sacrificing trust by requiring someone else to manage the keys.

Split Key encryption and homomorphic key encryption is used. Breakthrough split-key encryption technology protects keys and guarantees they remain under customer control and are never exposed in storage; and with homomorphic key encryption, the keys are protected – even while they are in use. Each data object (such as a disk or file) is encrypted with a unique key that is split in two. The first part – the master key – is common to all data objects in the application. It remains the sole possession of the application owner and is unknown to organization. The second part is different for each data object and is stored by the organization's Key Management

Service. Every time the application accesses the data store, organization uses both parts of the key to dynamically encrypt and decrypt the data. When the master key is in the cloud, it is homomorphically encrypted – even when in use – so that it can never be hacked or stolen.

II. PROPOSED METHODOLOGY

This paper provides a Split-Key encryption technology and homomorphic key encryption in cloud. The noteworthy term isn't encrypting the data– it's protecting the encryption keys. Every time an application accesses a data store, it needs to use the encryption keys. Virtual Key Management is the first solution to keep your cloud data truly secure.

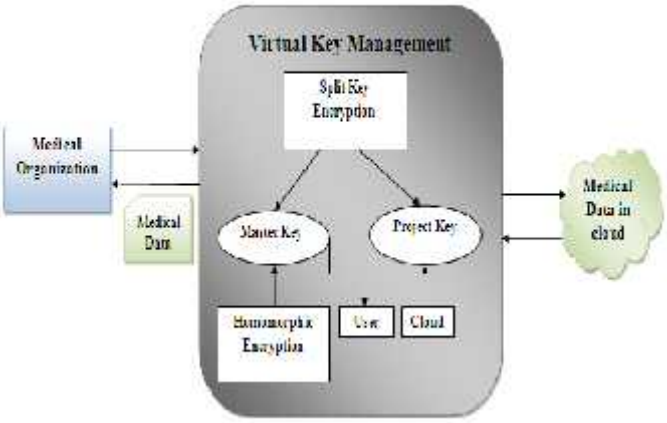

Figure: 1 Proposed Model

The proposed model is implemented by dividing into four phases. They are,

1. Key generation phase
2. Encryption phase
3. Decryption phase
4. Accessing secure data

1. Key Generation Phase

Split key encryption and Homomorphic encryption is used, where Two keys are generated in Split-key encryption. Each key has two parts:

- The first part, the Master Key, is retained by the application owner (you) and is never stored in open form in either your cloud account, or on the organization Key Management Server.
- The second part, the project key, is stored on the organization Key Management Service.

When the application needs to access the data store, the Virtual Key Management combines both parts of the key in a mathematical operation. Ordinarily, this would require both parts of the key to be exposed. However , both parts of the key are encrypted before and during the startup of the virtual appliance. As a result, the keys are fully encrypted when they are resident in your cloud account. Furthermore, Cloud organization encrypts the keys differently for every legitimate use. So even if your encrypted master key is stolen, it can never be used to access your data.

The master key is homomorphically encrypted. With Fully Homomorphic Encryption, all mathematical operations can be performed on encrypted data, but since it requires an enormous amount of computational resources, it isn't yet feasible for a real-world system. With Partially Homomorphic Encryption, only select mathematical operations are supported, dramatically reducing the computational overhead. The benefits are fast, reliable performance for your business-critical applications.

2. Encryption Phase

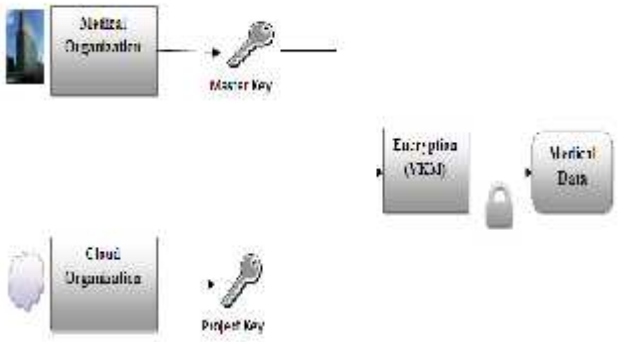

Figure : 2 Encryption Phase

Fig:2 shows that ,Medical organization i.e., the owner has to store their medical data of the organization in the cloud inorder to save the space, money and to secure the data even from the authorized person. In cloud, instead of encrypting data, the biggest challenge is encrypting the keys. Split Key technology is used for encryption which uses AES-256 algorithm. Split key technology has two keys. Medical organization owns the master key and the cloud organization has the project key. Both these keys are encrypted and the medical data has been locked.

3. Decryption Phase

Fig:3 shows that, when the application needs to access the data store, the Virtual Key Management combines both parts of the key. When there is a presence of both keys, the data

can be retrieved. The data cannot be retrieved with master key alone and similarly with project key.

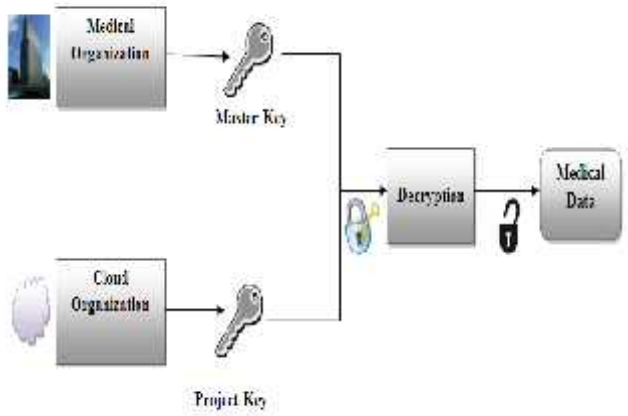

Figure : 3 Decryption Phase

3. Accessing Secure Data

The key has been generated and data is encrypted using Split-key encryption and Homomorphic encryption. Then the data and keys are encrypted. After encryption, When the application needs to access the data store, the Virtual Key Management combines both parts of the key in a mathematical operation. Ordinarily, this would require both parts of the key to be exposed. However , both parts of the key are encrypted before and during the startup of the virtual appliance. As a result, the keys are fully encrypted when they are resident in your cloud account. Furthermore, Cloud organization encrypts the keys differently for every legitimate use. So even if your encrypted master key is stolen, it can never be used to access your data. So the data is truly secure.

III.AES-256 ALGORITHM

The algorithm used in this paper is AES algorithm. The AES Algorithm[6] is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption and decryption. The data block length is fixed to be 128 bits, while the length can be 128,192,or 256 bits. In addition, the AES algorithm is an iterative algorithm. Each iteration can be called a round, and the total number of rounds is 10,12, or 14, when key length is 128,192, or 256, respectively. The 128 bit data block is divided into 16 bytes. These bytes are mapped to a 4x4 array called the State, and all the internal operations of the AES algorithm are performed on the State.

The encryption process is iterative in nature. Each iterations are known as rounds. For each round 128 bit input data and 128 bit key is required. That is, need 4 words of key in one round. So the input key must be expanded to the required number of words, which depends upon the number of rounds.

TABLE I
AES PARAMETERS

Algorithm	Key length (Nk words)	Block Size (Nb words)	Number of rounds (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

The output of each round serves as input of next stage. In AES system, same secret key is used for both encryption and decryption. So it provides simplicity in design.

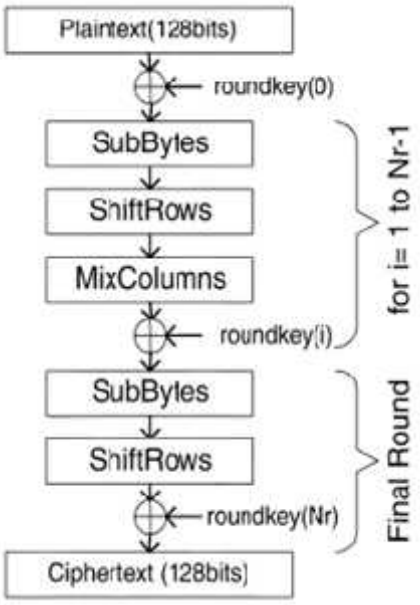

Figure:4 Detailed Block diagram of encryption part

In the encryption of the AES algorithm (Figure:4), each round except the final round consists of four transformations:

i. SubBytes: Operates in each byte of the State independently. Each byte is substituted by corresponding byte in the S-box.
ii. ShiftRow: Cyclically shifts the rows of the State over different offsets.
iii. MixColumn: In this operation the column of the State are considered as polynomials over GF(2^8) and are multiplied with a fixed polynomial. The MixColumn component does not operate in the last round of the algorithm.
iv. AddRoundKey: Involves bit-wise XOR operation.

Design steps

State array

The input to the encryption algorithm is a single 128-bit block. This block is copied into the State array, which is a square matrix of bytes. State array is modified at each stage of

encryption. Similarly, the 128 bit key is depicted as a square matrix of bytes. The ordering of bytes within a matrix is by column.

Key expansion

Key expansion is an important for both encryption and decryption. The AES key expansion algorithm takes as input a 4-word (16 bytes) key and produces a linear array of 44 words (176 bytes).This is sufficient to provide a 4-word round key for the initial Add Round Key stage and each of the 10 rounds of the cipher.

The following pseudocode describes the expansion:

```
KeyExpansion(byte key[16],word[44])
{
word temp
for (i=0; i<4; i++)
w[i]=(key[4*i],key[4*i+1],key[4*i+2],key[4*i+3]);for
(i=4; i<44; i++)
{
temp =w[i-1];
if(i mod 4 = 0)
temp=SubWord(RotWord(temp)) xor Rcon[i/4];
w[i] = w[i-4] xor temp
}
}
```

Table 2: Pseudocode for KeyExpansion

AddRound Key

The 128 bits of State array are bitwise XORed with the 128 bits of the round key(4 words of the expanded key).The operation is viewed as a column wise operation between the 4 bytes of the State array column and one word of the round key(Fig:5)

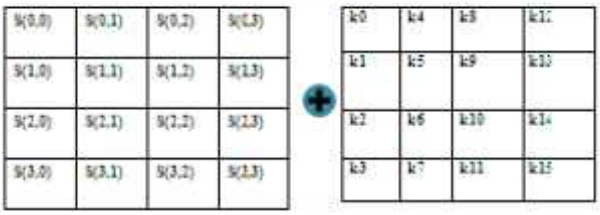

Figure 4: XOR operation between State and key word

IV CONCLUSION

Preserving security and privacy is a challenging issue in cloud. This paper makes a step forward in solving this issue by proposing Virtual Key Management technology which embeds Split Key encryption and Homomorphic encryption and has two keys: master key and project key. The efficiency of this technology guarantees better when compared with the existing one. The drawback of this technique is both the organization presents their presence at the time to retrieve the data. So delay may occur. So in future, this issue may resolved with an efficient encryption technology.

REFERENCES

[1]. H. J. Smith, S. J. Milberg, and S. J. Burke, "Information Privacy: measuring individuals' concerns about organizational practices," *MIS Q.*, vol. 20,pp. 167–196, Jun. 1996.

[2]. F. H. Simone, *IT-Security and Privacy: Design and Use of Privacy-Enhancing Security Mechanisms* (Lecture Notes in Computer Science Series). New York: Springer-Verlag, Jun. 2001, p. 6.

[3]. *http://www.luitinfotech.com/kc/what-is-cloud-computing.pdf*.

[4]. Chien-Ding Lee, Kevin I.-J. Ho, and Wei-Bin Lee, "A Novel Key Management Solution for Reinforcing Compliance With HIPAA Privacy/Security Regulations," IEEE Transactions On Information Technology In Biomedicine, Vol. 15, No. 4, July 2011.

[5]. Wawge P.U. and Rathod A.R., "Cloud Computing Security with Stegnography and Cryptography AES Algorithm Technology", World Research Journal of Computer Architecture", Volume 1, Issue 1, 2012, pp. -11-15.

[6]. P.Karthigaikumar,Soumiya Rasheed, "Simulation of Image Encryption using AES Algorithm", *IJCA Special Issue on Computational Science - New Dimensions & Perspectives"**NCCSE, 2011.***

[7]. M. Li, R. Poovendran, and S. Narayanan, "Protecting patient privacyagainst unauthorized release of medical images in a group communication environment," *Comput. Med. Imag. Graph.*, vol. 29, pp. 367–383, 2005.

[8]. R. Cushman, "Information and medical ethics: Protecting patient privacy," *IEEE Technol. Soc. Mag.*, vol. 15, no. 3, pp. 32–39, Fall 1996.

[9]. Bellare M. Desai A., Jokipii E. and Rogaway P. *Proc. Ann. Symp. Foundations in Computer Science* (*FOCS*), 394-403.

[10]. Bruce schneier"*Applied Cryptography*" 2nd Edition published by John Wiley&SonsInc.

[11]. William stallings "*Cryptography and Network Security*" 3rd Edition published by Pearson Education Inc and Dorling Kindersley Publishing Inc.