Security To The Healthcare Cloud Data Using Hybrid Approach

Nirali Kapadia[1], Prof. Ajaykumar T. Shah[2]
Department of Computer Engineering
[1]Assistant Professor, Alpha College of Engineering and Technology, Khatraj, Gandhinagar
[2]HOD, Alpha College of Engineering and Technology, Khatraj, Gandhinagar

Abstract*- Our work advocates the use of linear network coding and re-encryption based on ElGamal cryptography. To provide security and fault tolerance for cloud storage, we go for linear network coding. If a cloud suffers from a permanent failure and loses all its data, then we need to repair the lost data from other surviving clouds to preserve data redundancy. To exchange the encoding key matrix securely with the receiver, we go for ElGamal re-encryption scheme. We show how securely the data can be transferred between sender and the receiver. We also compare our coding scheme with the traditional replication scheme for achieving reliability.*

Keywords- Heat transfer, Nanofluid, Thermal Conductivity etc.

I. INTRODUCTION

Network coding is refer to coding at a node in a network, where coding is an arbitrary, casual mapping of inputs to outputs. Another possible definition of network coding, is coding at a node in a network with error-free links. This distinguishes the function of network coding from that of channel coding for noisy links; we can similarly distinguish the function of network coding from that of source coding by considering the former in the context of independent incompressible source processes. This definition is frequently used and, under it, the study of network coding reduces to a special case of network information theory. A third definition of network coding, then, is coding at a node in a packet network (where data is divided into packets and network coding is applied to the contents of packets), or more generally, coding above the physical layer. Network coding can improve: -

Throughput, **Robustness, Complexity and Security[1].**

Re-encryption allows a proxy to transform a cipher text computed under sender's public key into one that can be opened by receiver's secret key [15]. There are many useful applications of this primitive. For instance, Alice might wish to temporarily forward encrypted email to her colleague Bob, without giving him her secret key. In this case, Alice the sender could designate a proxy to re-encrypt her incoming mail into a format that Bob the receiver can decrypt using his own secret key [15].

How it can be done using ElGamal cryptography:

- Let p be a prime no.
- g be a generator of Zp = {0,…p-1}
- Let y = g^x (mod p), x is a randomly selected private key
- Thus the pubic key of ElGamal is a triplet {p,g,y}
- Private key = {x}
- Encryption:
- Generate random value k and encrypt plaintext M as follows:
- a <-- g^k (mod p)
- b <-- M*y^k (mod p)
- Thus encrypted text is (a,b).
- Decryption:
- The decryption of the cipher text C = (a,b) can be done by using following modular operation:
- M <-- b/a^x (mod p)
- For using ElGamal in proxy re encryption, the private key x is splitted into x1 and x2 such that x1 + x2 = x
- According to users requirement x2 is splitted into x3 and x4 such that x3 + x4 =x2
- If we have cipher text C then using x1 we can have another text say M1 such that M1 = b/a^{x1} (mod p)
- M1 can be converted into M2 such that M2 = b/a^{x3} (mod p)
- M2 can be converted into plaintext M such that
- M = b/a^{x4} (mod p)
- The correctness of proxy ElGamal encryption can be verified as follows:

$$M_2/a^{x4} \bmod p = (M_1/a^{x3} \bmod p)/a^{x4} \bmod p$$

$$= (b/a^{x1} \bmod p)/a^{x3 + x4} \bmod p$$

$$= (b/a^{x1} \bmod p)/a^{x2} \bmod p$$

$$= b/(a^{x1 + x2)} \bmod p$$

$$= b/a^{x} \bmod p$$

II. LITERATURE SURVEY

In [3], the author has proposed an efficient mechanism with silent features of data integrity and confidentiality. Here the author has used the concept of RSA, Hash function along with several cryptography tools. But a trusted third party is used where the data is present in unencrypted form. This is not suitable for healthcare data. All the computation and verification are offloaded to TPA so there is a need to make TPA more secure.

In [4], the author has introduced a third party auditor, who will on the behalf of user will check for data integrity of data stored on cloud server. A homomorphic encryption scheme is used to encrypt the data which will be shared with TPA. Elgamal homomorphic encryption will not allow TPA to learn anything about data content during auditing process. The drawback here is that the data is stored over the cloud server in the form of blocks and these blocks along with their metadata are in unencrypted form. So there is a data integrity and confidentiality risk over that data as Cloud Service Provider (CSP) is considered trustworthy.

In [5], the author has considered the problem of building a secure cloud storage service. A combination of RSA and AES encryption method is proposed to share the data among users in a secure cloud system. It provides difficulty for attackers as well as reducing the time of information transmission between user and cloud. The process of sending the files to the cloud and retrieving the files from the cloud was accomplished by symmetric and asymmetric encryption respectively. The drawback of the system is that the number of keys becomes triple for each file stored over the cloud. Moreover the encryption and decryption process that done twice for each file cause system overhead.

In [6], the author has designed a security framework for data privacy in healthcare system. It is based on web service architecture. The application is basically delivered via the internet through web browser. The data is processed and stored in the proper encrypted form. Despite this fact, it is a challenge because users have to rely on the service providers for the appropriate security. In addition, accessing the web application over the internet makes access from any device, information stealing in the intermediate state is a problem when the file is being encrypted.

In [7], the author presents a hybrid approach by using RSA and AES encryption algorithm to safeguard data security in Cloud. Security being the most important factor in cloud computing, this paper focuses on: 1) Secure Upload of data such that even administrator is unaware of the contents. 2) Secure download of data in such a way that the integrity of data is maintained. The drawback here is that the Cloud Service Provider is partially trusted which is not acceptable for healthcare data.

In [8], the author has proposed a “three way mechanism” to get rid of security issues such as authentication, data security and verification, at the same time. The author makes use of digital signature and Diffie-Hellman key exchange blended with AES (Advanced Encryption Standard) algorithm to protect confidentiality of data stored in cloud. Even if the key is transmission is hacked, the facility of Diffie Hellman key exchange render it useless, since key in transit is of no use without user’s private key, which is confined only to the legitimate user.

In [9], a novel encryption based scheme is proposed to support access control terminology. This is more elastic in nature, most mountable it is, and the most important fine grained access control is achieved through this scheme in cloud computing. We can see this scheme as a advancement of cipher text-policy attribute- set-based encryption (CPASBE) scheme. A hierarchical arrangement is illustrated which is more elastic, mountable in nature.

In [10], the author has proposed security scheme for mobile multicloud computing (MMC) and the data security from user side through homomorphic encryption. Homomorphic encryption claimed by many research as an optimal encryption for cloud computing environment. This paper prove the result performance in homomorphic encryption suitable for mobile multi-cloud computing. Future works for the researcher in this paper is improving the performance security aspects in mobile multi cloud computing and improve the encryption itself and research for the space or memory consumption for mobile environment.

In [11], the author has proposed commutative encryption which is a kind of an encryption system that enables a plaintext to be encrypted more than once using different users’ public keys. In this system, decryption is not required before the encryption/re-encryption processes. Moreover, the resulted cipher text can be decrypted by the designated decrypters without considering the order of public keys used in the encryption/re-encryption processes. In other words, the order of keys used in encryption and in decryption do not affect the computational result. In this paper, the author propose a new commutative encryption scheme based on the ElGamal encryption and provide the security proof in the random oracle model.

In [12], the author has mainly analysed several different construction patterns of cloud computing, and quite relevant case in the deployment construction security of cloud computing by fit and unfit quality, and proposed finally an optimization safe deployment construction of cloud computing and security mechanism of material protection calculating method, namely, Global Authentication Register System (GARS), to reduce cloud material outflow risk. We implemented a system simulation to test the GARS algorithm of availability, security and performance. By experimental data analysis, the solutions of cloud computing security, and privacy derived from the research can be effective protection in cloud information security. Moreover, we have proposed cloud computing in the information security-related proposals that would provide related units for the development of cloud computing security practice.

In [13], a methodical approach to maintain security of the PHRS is proposed. PHRS helps the medical field a lot, patients and medical centres doesn't have to maintain separate record system of their own, they can store the information collectively in one cloud based centralized system known as Cloud PHRS. As there is role of cloud in such systems, the stored data security will be our major concern. To overcome that we proposed proxy re-encryption scheme involving PKG which generates all the three keys (two private keys for each user at two ends and proxy re-encryption key), proxy cloud which uses PKG to transform the encryption, the same method can be extended for large medical distributed system.

The above discussion concludes that there have been very less work done in the field which involves security and reliability of data at the same time. So, we focused on this two parameters for our work. We have concluded after literature study that the best strategy to provide security to data is to use symmetric and asymmetric algorithms on the data at same time. The reason behind it is that Symmetric algorithm takes less amount of time in cryptographic operations compared to asymmetric algorithm. Thus we can encrypt our original data first by using symmetric algorithm and the key that we used to encrypt the data can be encrypted by asymmetric algorithm.

Proposed Architecture:

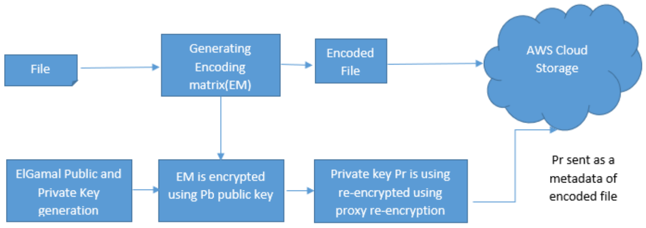
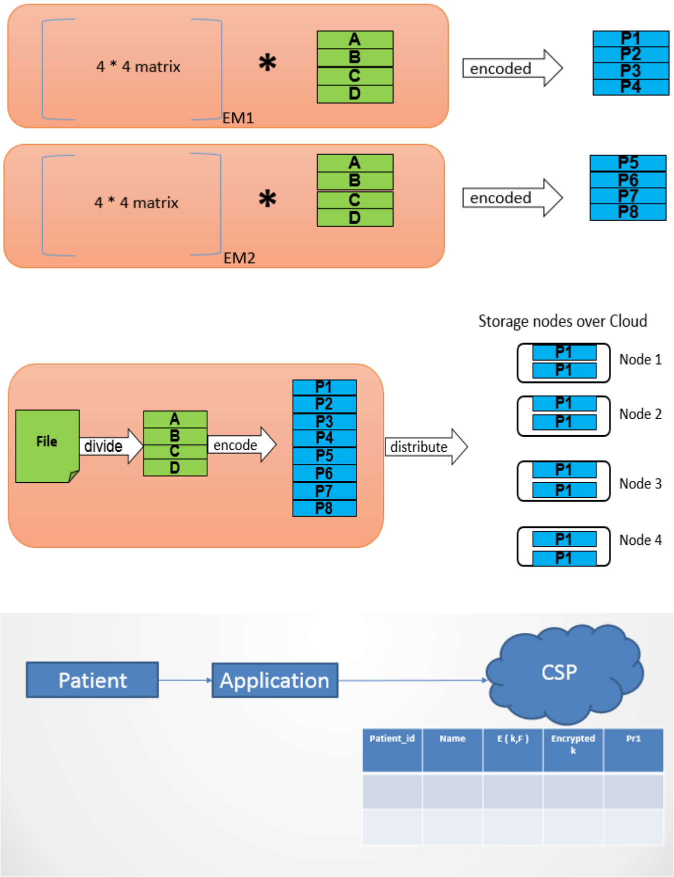

File
Generating Encoding matrix(EM)
Encoded File
AWS Cloud Storage
ElGamal Public and Private Key generation
EM is encrypted using Pb public key
Private key Pr is using re-encrypted using proxy re-encryption
Pr sent as a metadata of encoded file

Figure 1. Proposed Architecture

The work is divided into 4 modules:

- 1) Secure Data Storage
- 2) Secure Data Sharing
- 3) Secure Data Access
- 4) Secure Access Revocation

1) Secure Data Storage



Patient_id	Name	E (k,F)	Encrypted k	Pr1

Figure 2. Working of secure data storage

- Network coding matrix EM1 and EM2 is generated.
- File F is encoded using key EM1. **Encode(F,EM1)**
- File F is encoded using key EM2. **Encode(F,EM2)**
- Encoding Matrix EM = {EM1 , EM2}
- ElGamal generates public key Pb and private key Pr.
- Network coding matrix EM is encrypted using public key Pb of ElGamal.

E(EM,Pb)

- Private Key Pr is partitioned into 2 random parts Pr1 + Pr2 = Pr.
- EM is partially decrypted using Pr1. **D(E (EM , Pb), Pr1)**
- Encoded Files and partially decrypted EM is sent to the cloud for storage.
- Encoded files are P1,……P8.

- The partially decrypted encoding matrix EM will be sent along with all this files as a metadata of the file.

2) Secure Data Sharing

- When the doctor wants to download data, he makes request to the patient.
- Pr2 will be partitioned into two random parts. Such that Pr2 = Pr3 + Pr4
- Pr3 will be send to the storage node and will be stored as a metadata.
- The proxy will turn partially decrypted EM into another form using Pr3.
- Pr4 is send to the intended doctor.

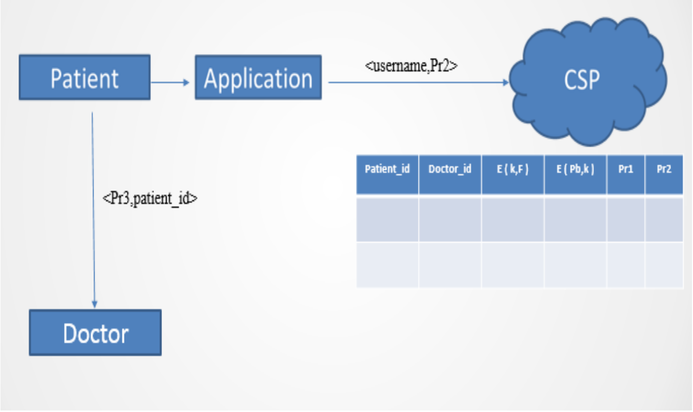


Figure 3. Working of secure data sharing

3) Data Access and Revocation

Data Access:

- Doctor will enter the user ID as well as patient ID and cloud will return any 4 files which will have the partially decrypted encoding matrix EM.
- Using Pr4 symmetric key will be decrypted. **D(D(D(E(EM , Pb),Pr1),Pr3),Pr4) = EM**
- Using inverse of EM , file F will be decrypted. **Decode(F,EM)**

Access Revocation:

- When the patient decides to revoke a specific data from access to his e-health data, the patient simply calls the CSP to delete the receiver’s partial key entry. If the doctor attempts to download the data from the CSP, he will only see the encoded file since the network coding key will never be decrypted.

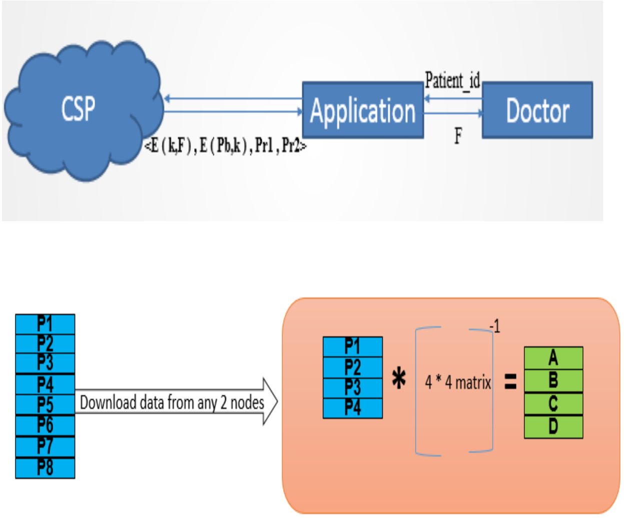


Figure 4. Working of secure data access and revocation

- If the original file has n blocks of original data, then by downloading n blocks, instead of 2n blocks, we could get the original data blocks, by using inverse of the encoding matrix.

Reliability Proof using NC:

- Example proving reliability using Network coding:
- Suppose we have data [1 2] , then to do network coding over this data we need two 2*2 matrices as key matrix.
- $\begin{matrix}1 & 2\end{matrix} \quad * \quad \begin{matrix}1 & 2\\ 3 & 4\end{matrix} \quad = \quad \begin{matrix}7 & 10\end{matrix}$
- $\begin{matrix}1 & 2\end{matrix} \quad * \quad \begin{matrix}3 & 4\\ 9 & 6\end{matrix} \quad = \quad \begin{matrix}21 & 16\end{matrix}$
- Then we have encoded data as [7 10 21 16] out of the original data [1 2]
- If the lost data is [7 21], then we could obtain the original data [1 2] from the data [10 16]
- $\begin{matrix}10 & 16\end{matrix} \quad * \quad \text{inverse of} \quad \begin{matrix}2 & 4\\ 4 & 6\end{matrix} \quad = \quad \begin{matrix}1 & 2\end{matrix}$

III. EXPERIMENTAL RESULTS AND ANALYSIS

The experiment is carried out on the machine that have following configuration:

Processor: Intel(R) Core(TM) i5-2467M CPU @1.60GHz

RAM: 4.00 GB

System Type: 32-bit OS

Windows: 8 Pro

The software used for the implementation are:

Eclipse kepler version 4.3

JDK 1.8

AWS SDK for Eclipse

Amazon Web Services:

We have implemented our work over AWS cloud services. **Amazon Web Services** (**AWS**), is a subsidiary of Amazon.com, which offers a suite of cloud computing services that make up an on-demand computing platform. These services operate from 12 geographical regions across the world. The most central and best-known of these services arguably include Amazon Elastic Compute Cloud, also known as "EC2", and Amazon Simple Storage Service, also known as "S3". AWS now has more than 70 services that span a wide range including compute, storage, networking, database, analytics, application services, deployment, management, mobile, developer tools and tools for the Internet of things.

We have made the use of Amazon Simple Storage Service, also known as "S3" services of AWS. The steps are shown below how we can use S3 services:

[1] Download AWS S3 SDK
[2] Configure it in Eclipse EE. We have used Eclipse Kepler version 4.3
[3] Downloading S3 API for Java
[4] Creating Bucket across any region of the AWS Server
[5] Applying the Proposed algorithm over the file
[6] Adding the Metadata to the file, which contains the partially decrypted key.
[7] Upload the file along the Metadata over S3.

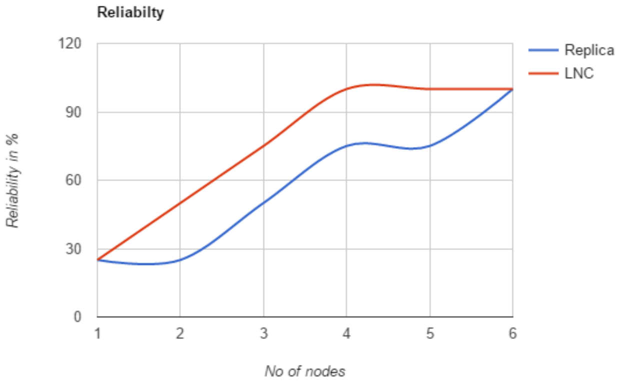


Figure 5. Comparision graph

The above graph shown in graph represents that by using Linear Network encoding (LNC) approach we could always recover more amount of data compared to the nodes recovered using traditional replication approach.

IV. CONCLUSION AND FUTURE WORK

In our work, we proposed the use of linear network coding and re-encryption based on ElGamal cryptography. To provide security and fault tolerance for cloud storage, we go for linear network coding. If a cloud suffers from a permanent failure and loses all its data, then we need to repair the lost data from other surviving clouds to preserve data redundancy. To exchange the encoding key matrix securely with the receiver, we go for ElGamal re-encryption scheme. We have shown how securely the data can be transferred between sender and the receiver. We also compare our coding scheme with the traditional replication scheme for achieving reliability.

Our work can be extended for achieving the reliability of multimedia data. We have worked upon the text data only. But this work can be extended for audio and video data over the cloud using the concept of P-Frame, B-Frame and I-Frame. We can also work upon reducing the complexity of the operation carried out for achieving security and reliability of data.

REFERENCES

[1] G. Rathi, Abinaya. M, Deepika. M¸ Kavyasri. T. “ Healthcare Data Security in Cloud Computing”, IJIRCCE 2015
[2] Zhang, Yin, et al. "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data." (2015).
[3] Garg, Parul, and Vishal Sharma. "An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function." Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on. IEEE, 2014.
[4] Rewadkar, D. N., and Suchita Y. Ghatage. "Cloud storage system enabling secure privacy preserving third party audit." Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on. IEEE, 2014.
[5] Khanezaei, Nasrin, and Zurina Mohd Hanapi. "A framework based on RSA and AES encryption algorithms for cloud computing services." Systems, Process and Control (ICSPC), 2014 IEEE Conference on. IEEE, 2014.
[6] Thiranant, Non, Mangal Sain, and Hoon Jae Lee. "A design of security framework for data privacy in e-health system using web service." Advanced Communication

Technology (ICACT), 2014 16th International Conference on. IEEE, 2014.

[7] Mahalle, Vishwanath S., and Aniket K. Shahade. "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm."Power, Automation and Communication (INPAC), 2014 International Conference on. IEEE, 2014.

[8] Mahalle, Vishwanath S., and Aniket K. Shahade. "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm."Power, Automation and Communication (INPAC), 2014 International Conference on. IEEE, 2014.

[9] Gupta, Suneet K., Seema Rawat, and Pranaw Kumar. "A novel based security architecture of cloud computing." Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on. IEEE, 2014.

[10] Louk, Maya, and Hyotaek Lim. "Homomorphic encryption in mobile multi cloud computing." Information Networking (ICOIN), 2015 International Conference on. IEEE, 2015.

[11] Huang, Kaibin, and Raylin Tso. "A commutative encryption scheme based on ElGamal encryption." Information Security and Intelligence Control (ISIC), 2012 International Conference on. IEEE, 2012.

[12] Chen, Chih-Yung, and Jih-Fu Tu. "A Novel Cloud Computing Algorithm of Security and Privacy." Mathematical Problems in Engineering 2013.

[13] E. Sathiyamoorthy, K. Govinda and Sathiyamoorthy. "Securing Healthcare Records Using Proxy Re-Encryption Scheme in Cloud."2014.

[14] Sipos, Márton, et al. "Distributed cloud storage using network coding."Consumer Communications and Networking Conference (CCNC), 2014 IEEE 11th. IEEE, 2014.

[15] Ahlswede, Rudolf, et al. "Network information flow." Information Theory, IEEE Transactions on 46.4 (2000).

[16] Heide, Janus, et al. "Network coding for mobile devices-systematic binary random rateless codes." Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference on. IEEE, 2009.

[17] Ho, Tracey, et al. "A random linear network coding approach to multicast."Information Theory, IEEE Transactions on 52.10 (2006).

[18] Meier, Andreas V. "The ElGamal Cryptosystem." (2005).

[19] Fitzek, Frank HP, et al. "Implementation and performance evaluation of distributed cloud storage solutions using random linear network coding." Communications Workshops (ICC), 2014 IEEE International Conference on. IEEE, 2014.

[20] Hu, Yuchong, et al. "NCCloud: applying network coding for the storage repair in a cloud-of-clouds." FAST. 2012.

[21] Fragouli, Christina, Jean-Yves Le Boudec, and Jörg Widmer. "Network coding: an instant primer." ACM SIGCOMM Computer Communication Review 36.1 2006.