Securing Healthcare Information over Cloud Using Hybrid Approach

Kirit J. Modi and Nirali Kapadia

Abstract Cloud computing has increased the attention for accessing and storing information. To share and store healthcare information over Cloud is playing crucial role to provide cost-effective and flexible and reliable solution to the users. Despite advantages of Cloud-based Healthcare system, security of data is major factor, which restricts the acceptance of the Cloud-based model. As a solution to the security challenge, our work advocates the use of linear network coding and re-encryption based on ElGamal cryptography in the form of hybrid approach to secure healthcare information over cloud. To provide security and fault tolerance for cloud storage, we have considered linear network coding mechanism. To exchange the encoding key matrix securely with the receiver, ElGamal re-encryption scheme is used. As a proposed approach, we present how securely the data can be transferred between sender and the receiver over cloud.

Keywords Cloud computing · Linear network encoding · Proxy re-encryption ElGamal cryptography

1 Introduction

Cloud computing is gaining popularity as an emerging technology for sharing the resources over the Internet. Cloud computing provides flexibility, reliability, sustainability and cost effectiveness to the users. For existing healthcare systems, there

K. J. Modi (✉)
Department of Information Technology, U. V. Patel College of Engineering, Ganpat University, Gujarat, India
e-mail: kiritmodi@gmail.com

N. Kapadia
Department of Computer Engineering, U. V. Patel College of Engineering, Ganpat University, Gujarat, India
e-mail: niralijollykapadia@gmail.com

C. R. Panigrahi et al. (eds.), *Progress in Advanced Computing and Intelligent Engineering*, Advances in Intelligent Systems and Computing 714,
https://doi.org/10.1007/978-981-13-0224-4_6

is a key requirement to develop an approach that minimizes time-consuming work and expensive means to access a patient's medical record and integrating this changing set of medical information consistently to deliver it to the healthcare organization. Nowadays, healthcare providers have adopted the cloud platform that can perform their operations more efficiently. Cloud computing service enables a group of doctors to obtain an access to a patient's health record anytime, anywhere. Despite all the these advantages cloud computing provides to the healthcare systems, data security is among the major concerns, which make healthcare system move slowly towards the acceptance of Cloud-based healthcare technologies. Cloud computing benefits come at a cost of the emergence of various risks related to the information security that must be cautiously addressed. As a solution, we contribute our work as follows.

(i) To present the effective approach for securing the healthcare information over the cloud.
(ii) To perform the experimental work with the proposed approach and provide the results in the form of reliable solution.

The rest of this paper is organized as follows: in Sect. 2, we present the concepts of network encoding and proxy re-encryption using ElGamal cryptography. Section 3 discusses literature review related to secure healthcare system over the cloud. Section 4 proposes Cloud-based secure healthcare framework. Finally, Sect. 5 presents experimental work and results. Section 6 concludes this paper and discusses our future direction.

2 Background Concepts

In this section, we define network encoding [1] and Proxy re-encryption [2] using ElGamal cryptography concepts.

2.1 Network Coding

It is a technique in which coding is done at the nodes in a network. Network encoding is used to minimize the network delays and maximize the throughput of the network and make the network reliable and robust. Network encoding is used in the packet networks (where data is first fragmented into packets then transmitted to the destination). The network encoding is applied at the packets, so we can say that coding is done above the physical layer. Network coding improves the robustness, throughput, security and complexity of the network.

2.2 *Proxy Re-encryption*

It is technique which allows proxy to convert the cipher text generated by the sender's public key into such a form that can be decrypted by receiver's private key (without using sender's private key). There are many applications where we require proxy re-encryption. For example, Alice wants to send an encrypted email to Bob, without sharing her private key. In this case, Alice the sender uses a proxy re-encryption technique to re-encrypt the mail into a form that Bob the receiver can decrypt by using his own private key.

2.2.1 Proxy Re-encryption Using ElGamal Cryptography

The following steps show how we can perform Proxy re-encryption using ElGamal cryptography.

- Let us consider p be a prime number
- Let us consider g be a generator of $Zp = \{0, \ldots p - 1\}$
- Let $y =$ (mod p), where x is a randomly selected private key
- Thus, the pubic key of ElGamal is a triplet $\{p, g, y\}$
- Private key = $\{x\}$

(a) **Encryption**
Generate a random value k and encrypt plaintext M as follows:

- $a =$ (mod p)
- $b = M*$(mod p)
- Thus, encrypted text is (a,b)

(b) **Decryption**
The cipher text $C = (a,b)$ is decrypted by using following modular operation:

- $M = b/a^{x}$(mod p)
- For using ElGamal in proxy re-encryption, the secrete key x is splitted into x1 and x2,
- such that $x1 + x2 = x$
- According to user's 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 $M1 = b/a^{x1}$
- M1 can be converted into plaintext 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:

$$\begin{aligned}
M_2/a^{x4} \bmod p &= \left(M_1/a^{x3} \bmod p\right)/a^{x4} \bmod p \\
&= \left(b/a^{x1} \bmod p\right)/a^{x3+x4} \bmod p \\
&= \left(b/a^{x1} \bmod p\right)/a^{x2} \bmod p \\
&= \left(b/a^{x1} \bmod p\right)/a^{x2} \bmod p \\
&= b/\left(a^{x1+x2}\right) \bmod p \\
&= b/a^{x} \bmod p
\end{aligned}$$

3 Literature Study

The following section presents the literature related to the security aspects for healthcare information over cloud.

Garg, Parul, and Vishal Sharma [3] have proposed an efficient mechanism to store data securely in cloud. Here the author uses RSA and Hashing cryptography tools to securely store data in cloud. 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.

Rewadkar, D. N., and Suchita Y. Ghatage [4] have introduced a third-party auditor, who checks the integrity of data in cloud storage on the behalf of cloud customer. Before sharing the data with TPA, the data is encrypted by using homomorphic encryption method. During auditing process, TPA will know able to know anything about the data stored in cloud. 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 data integrity and confidentiality risk over that data as Cloud Service Provider (CSP) is considered trustworthy.

Khanezaei Nasrin and Zurina Mohd Hanapi [5], proposed a method in which they used the combination of RSA and AES encryption method to securely share data stored in cloud. Symmetric and asymmetric encryption respectively is used for both uploading and downloading file from cloud. The main drawback of system is that we have to do encryption and decryption twice for the same file stored in cloud which cause the overhead for the system.

Thiranant et al. [6] has designed a framework which provides security to e-healthcare system. This framework uses web services to provide security to the data stored in cloud. The application can be access through browser via the Internet. The data are stored in cloud is encrypted, but for security we have to trust on service providers. Since the system is accessed via internet stealing of data is one of the major challenges in such systems.

In [7], the author presents a hybrid approach by using RSA and AES encryption algorithm to securely store data in cloud server. In cloud system security is one of the biggest issues in this paper author focus on: (1) securely upload the data to cloud in such way that even administrator does not know about the contents. (2) Securely download the data from cloud in such a way that the data integrity is not affected. The drawback here is that the cloud service provider is partially trusted which is not acceptable for healthcare data.

In [7], the author has designed a "three-way mechanism" to increase the security in cloud by using AES and Diffie-Hellman key exchange algorithm and digital signature. In this mechanism author uses Diffe-Hellman key exchange thus if key is hacked while transmission it is useless to hacker because hacker doesn't have legitimate user's private key.

Gupta, Suneet K., Seema Rawat, and Pranaw Kumar [8] proposed a novel security architecture for access control in cloud computing. This scheme is advancement in CPASBE (cipher text-policy attribute-set-based encryption) scheme.

Louk, Maya, and Hyotaek [9] proposed a data security scheme for mobile multicloud computing (MMC) homomorphic encryption. This paper proves that homomorphic encryption is optimal for mobile multicloud computing. Improving security and performance is one of the future aspects for other researchers.

In [10], the author proposed a commutative encryption method based on the ElGamal encryption in which a plaintext is encrypted more than one time using different users' public keys. In this system, the computational result is not affected by the order of keys used in encryption and decryption.

In [11], the author proposed a novel Global Authentication Register System (GARS) to provide security in cloud system. They implemented the GARS algorithm in simulation environment and by analyzing the experimental result they show that their system provides effective security to cloud system.

In [12], author proposed an approach to provide security to cloud-based healthcare system. The patients and medical centers can store in cloud based centralized system. When data is stored in cloud security is one of the major issue thus to overcome that they use proxy re-encryption scheme in which allows proxy to convert the cipher text generated by the sender's public key into a such a form that can be decrypted by receiver's private key (without using sender's private key).

The above discussion concludes that there has been very less work done in the field which involves security and reliability of data at the same time. So, we focused on these 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.

4 Proposed Work

In this section, we presented our proposed architecture and approach for Securing healthcare information over cloud.

4.1 *Cloud-Based Secure Healthcare Information System*

In Fig. 1, we have proposed framework for security to the healthcare information over Cloud which is divided into four main modules as follows. The functionality of each module is discussed here.

The framework is divided into four modules.

I. **Secure Data Storage**

Secure data storage process using network coding technique is defined as follows which is presented in Figs. 2 and 3 as follows.

- 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 is partitioned into two 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.

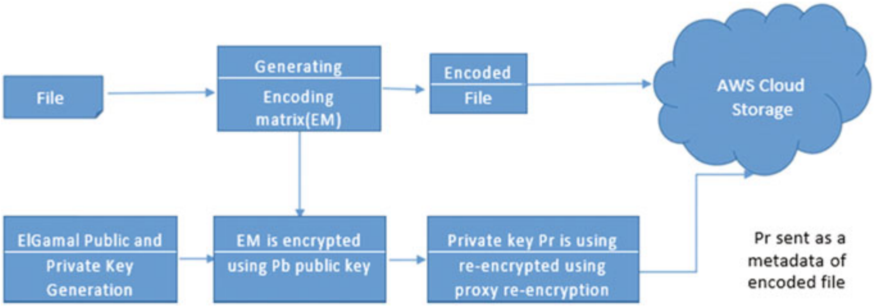


Fig. 1 Proposed framework of cloud-based secure healthcare system

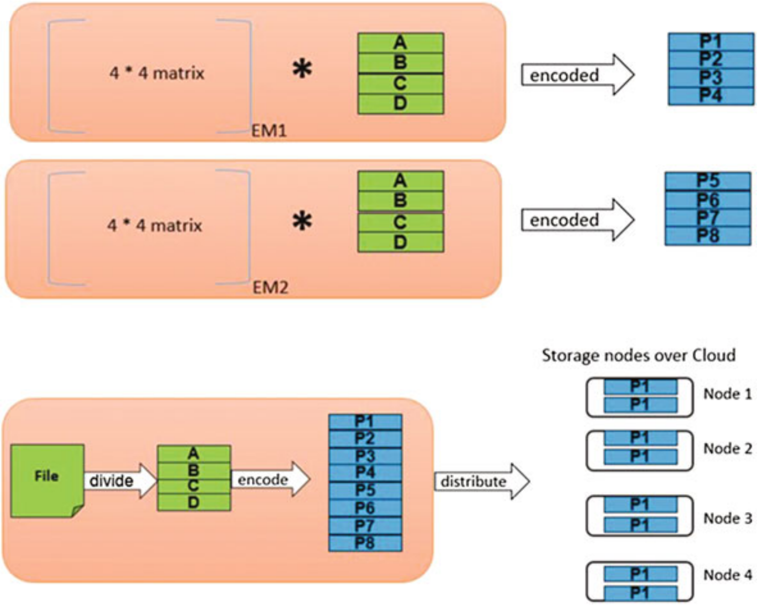
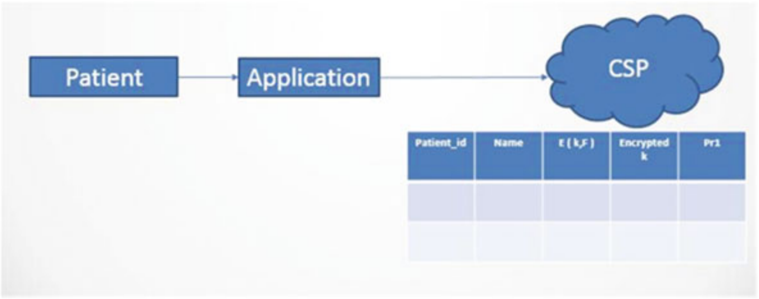


Fig. 2 Network coding



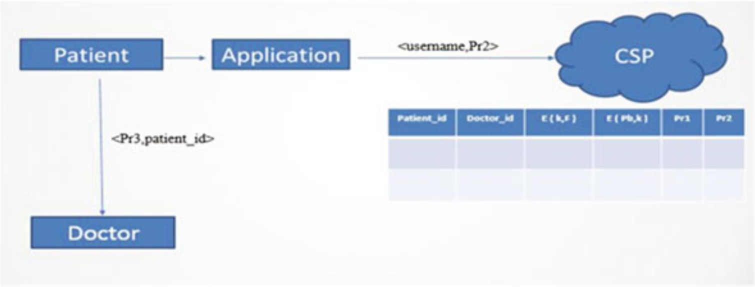
Patient_id	Name	E (k,F)	Encrypted k	Pr1

Fig. 3 Secure data storage

II. **Data Sharing**

Data sharing process is defined as follows which is presented in Fig. 4.

- 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 sent 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.



Patient_id	Doctor_id	E (k,F)	E (Pb,k)	Pr1	Pr2

Fig. 4 Data sharing

III. **Data Access**

Data access process is defined as follows:

- Doctor will enter the user ID as well as patient ID and cloud will return any 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).

IV. **Access Revocation**

Access revocation process is defined as follows which is presented in Fig. 5.

- When the patient wishes to withdraw 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 downloads the data from the CSP, he will only get the encoded file since the network coding key will never be decrypted.

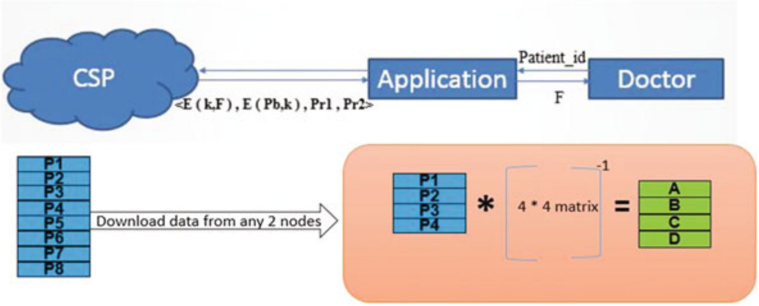


Fig. 5 Access revocation

- 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.

4.2 Reliability Proof Using Network Coding

Following example provides proof of 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.

$$\begin{matrix} 1 & 2 \end{matrix} \; * \; \begin{matrix} 1 & 2 \\ 3 & 4 \end{matrix} \; = \; \begin{matrix} 7 & 10 \end{matrix}$$

$$\begin{matrix} 1 & 2 \end{matrix} \; * \; \begin{matrix} 3 & 4 \\ 9 & 6 \end{matrix} \; = \; \begin{matrix} 21 & 16 \end{matrix}$$

- 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]

$$\begin{matrix} 10 & 16 \end{matrix} \; * \; \text{inverse of} \begin{matrix} 2 & 4 \\ 4 & 6 \end{matrix} = \; \begin{matrix} 1 & 2 \end{matrix}$$

5 Experimental Work and Results

The experiment is carried out on the machine having following configuration: Processor: Intel(R) Core(TM) i5-2467 M CPU @1.60 GHz, RAM: 4.00 GB, System Type: 32-bit OS Windows 8. The tools used for the implementation are: Eclipse kepler version 4.3, JDK 1.8, AWS SDK for Eclipse. We have implemented our work over AWS cloud services. Amazon Web Services (AWS), is one of the most popular cloud computing platform owned by Amazon. AWS offers different cloud computing solution that can be operated from 12 different geographical locations across the world. The well-known cloud services provided by Amazon are Amazon Simple Storage Service, also known as “S3” and Amazon Elastic Compute Cloud, also known as “EC2”. AWS provides more than 70 cloud services such as storage, computing, networking, database, developer tools for Internet of Things mobile development tools, application services, etc. We have made the use of Amazon Simple Storage Service, also known as “S3” services of AWS.

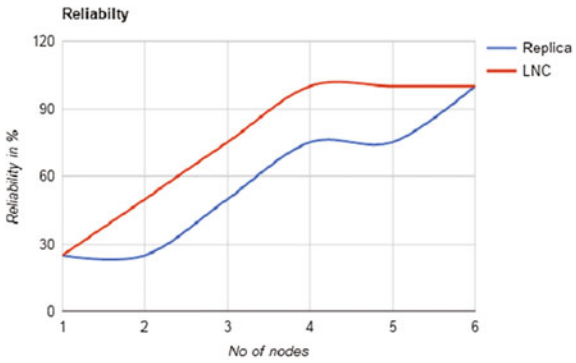


Fig. 6 Comparison of reliability gained using LNC and replication

The steps are shown below how we can use S3 services

- Download AWS S3 SDK.
- Configure it in Eclipse EE. We have used Eclipse Kepler version 4.3.
- Downloading S3 API for Java.
- Creating Bucket across any region of the AWS Server.
- Applying the Proposed algorithm over the file.
- Adding the Metadata to the file contains the partially decrypted key.
- Upload the file along the Metadata over S3.

5.1 Comparison of Proposed LNC with Replication Approach

A comparative illustration has been depicted in Fig. 6 by considering number of nodes from 1 to 6. The level of reliability is increased with increased number of nodes.

The above results represent 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.

6 Conclusion and Future Work

In this paper, we proposed hybrid approach using linear network coding and re-encryption based on ElGamal cryptography to secure healthcare information over the cloud. To provide security and fault tolerance for cloud storage, linear network coding is used. To exchange the encoding key matrix securely with the receiver, we have used ElGamal re-encryption scheme. We have presented how securely the data can be transferred between sender and the receiver. We also compared our coding scheme with the traditional replication scheme for achieving reliability. In this work, We have considered text data only.

As a future plan, this work could be extended for audio and video data over the cloud using the concept of P-Frame, B-Frame, and I-Frame. We could also work upon reducing the complexity of the operation carried out for achieving security and reliability of data.

References

1. Rathi G., Abinaya M., Deepika. M., Kavyasri. T.: Healthcare Data Security in Cloud Computing, IJIRCCE (2015).
2. Ahlswede, R., Cai, N., Li, S. Y., & Yeung, R. W.: Network information flow. Vol. 46 No. 4 IEEE Transactions on information theory (2000).
3. Garg, P., & Sharma, V.: An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function. In Issues and Challenges in Intelligent Computing Techniques (ICICT) International Conference on IEEE (2014).
4. Rewadkar, D. N., & Ghatage, S. Y.: Cloud storage system enabling secure privacy preserving third party audit. In Control, Instrumentation, Communication and Computational Technologies (ICCICCT), International Conference on IEEE (2014).
5. Khanezaei, N., & Hanapi, Z. M.: A framework based on RSA and AES encryption algorithms for cloud computing services. In Systems, Process and Control (ICSPC), 2014 IEEE Conference on IEEE (2014).
6. Thiranant, N., Sain, M., & Lee, H. J.: A design of security framework for data privacy in e-health system using web service. In Advanced Communication Technology (ICACT), 2014 16th International Conference on IEEE (2014).
7. Mahalle, V. S., & Shahade, A. K.: Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. In Power, Automation and Communication (INPAC), 2014 International Conference on IEEE (2014).
8. Gupta, S. K., Rawat, S., & Kumar, P.: A novel based security architecture of cloud computing. In Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), 2014 3rd International Conference on IEEE (2014).
9. Louk, M., Lim, H.: Homomorphic encryption in mobile multi cloud computing. In Information Networking (ICOIN), 2015 International Conference on IEEE (2015).
10. Huang, K., & Tso, R.: A commutative encryption scheme based on ElGamal encryption. In Information Security and Intelligence Control (ISIC), 2012 International Conference on IEEE (2012).
11. Chen, C. Y., & Tu, J. F.: A novel cloud computing algorithm of security and privacy. Mathematical Problems in Engineering (2013).
12. Govinda, K.: Secure Framework for cloud environment in collaboration with customers (2015).
13. Zhang, Y., Qiu, M., Tsai, C. W., Hassan, M. M., & Alamri, A.: Health-CPS: Healthcare cyber-physical system assisted by cloud and big data (2015).
14. Sipos, M., Fitzek, F. H., Lucani, D. E., & Pedersen, M. V.: Distributed cloud storage using network coding. In Consumer Communications and Networking Conference (CCNC). IEEE (2014).
15. Heide, J., Pedersen, M. V., Fitzek, F. H., & Larsen, T.: Network coding for mobile devices-systematic binary random rateless codes. In Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference on IEEE (2009).

16. Ho, T., Médard, M., Koetter, R., Karger, D. R., Effros, M., Shi, J., & Leong, B.: A random linear network coding approach to multicast Vol. 52 No. 10. IEEE Transactions on Information Theory (2006).
17. Meier, A. V.: The elgamal cryptosystem (2005).
18. Fitzek, F. H., Toth, T., Szabados, A., Pedersen, M. V., Lucani, D. E., Sipos, M., Medard, M.: Implementation and performance evaluation of distributed cloud storage solutions using random linear network coding. In Communications Workshops (ICC), 2014 IEEE International Conference on IEEE (2014).
19. Hu, Y., Chen, H. C., Lee, P. P., & Tang, Y.: NCCloud: applying network coding for the storage repair in a cloud-of-clouds. In FAST (2012).
20. Fragouli, C., Le Boudec, J. Y., & Widmer, J.: Network coding: an instant primer Vol. 36. No. 1 ACM SIGCOMM Computer Communication Review (2006) 63–68.