IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-8, Aug 2019 E-ISSN: 2347-2693

Improving Security for Data Migration in Cloud Computing using Randomized Encryption Technique

Akanksha Aasarmya[1*], Sohit Agarwal[2]

[1,2]Center of Cloud Infrastructure & Security, Gyan Vihar University, Jaipur, India

Corresponding Author: akanksha23995@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i8.3943 | Available online at: www.ijcseonline.org

Accepted: 16/Aug/2019, Published: 31/Aug/2019

***Abstract*—** Cloud computing is an increasingly famous and growing technology which has led to a new dawn in the field of Information Technology. It has created a drastic change in the trend of different digital devices. Cloud Computing corresponds to both, the applications provided as services over the internet and the hardware elements and systems software in the data-centers that provide those respective services. In this paper, improving the security of data within the cloud when the data is migrated from one source to cloud or vice-versa, using an enhanced randomized encryption technique. During the analysis of providing security to a large amount of data in the cloud environment using various encryption techniques, we formulated that the asymmetric algorithms are incapable to encrypt a data in a bulk or in large amount when used singly. Security is the major issue in cloud computing system so we are using the concept of asymmetric algorithm when we are migrating one source file to the cloud.

***Keywords*—**Cloud computing, Software as a services, Encryption, Asymmetric algorithms, RSA, AES

I. INTRODUCTION

These services themselves are being referred to as Software as a Service (SaaS). The data-centre hardware and software as a whole is what we will refer to as a Cloud. The consumer can access the service related to computer, whether it is a software or hardware or infrastructure, and pay for the respective duration he accessed that particular services, that is, "Pay as per Usage". With the help of this technology, the users don't have to invest in loads or find difficulties in the set up and maintenance the complex IT Infrastructure.

Cloud Computing corresponds to both, the applications provided as services over the internet and the hardware elements and systems software in the data-centre that provide those respective services. These services themselves are being referred to as Software as a Service (SaaS). The data-centre hardware and software as a whole is what we will refer to as a Cloud. The consumer can access the service related to computer, whether it is a software or hardware or infrastructure, and pay for the respective duration he accessed that particular services, that is, "Pay as per Usage". With the help of this technology, the users don't have to invest in loads or find difficulties in the set up and maintenance the complex IT Infrastructure. The name, cloud, is given due to the involvement of internet which is a metaphor of internet. The main advantage of cloud computing is that it reduces the cost and complexity of buying for good; configuring and managing all the hardware and software required for the application. Now, anyone in the world with an active internet connection can build powerful stand-alone applications with the services and features provided by Cloud Computing. Cloud Computing architecture allows users to make use of IT hardware and software in a better and efficient way. It increases the overall gain by improving resource utilization at its whole. Resources sharing from large pool of cloud pulls down cost and increases utilization by delivering resources only for as long as those resources are required.

i. Data migration in cloud computing:

The object of an organization can be moved from the cloud to cloud or data from one cloud to another. However, this is a very challenging task for migrating data and includes various key security issues such as data integrity, security, portability, data privacy, data accuracy, etc. To achieve an automatic data migration, a programmatic data migration approach is required to get rid of the tedious tasks of a human organization.

ii. Encryption: A Cryptographic approach for data security

Cryptography is a technique or science to secure sensitive data or information over an insecure network which involves the methods like conversion of the original text or information into cipher text known as ***Encryption*** and

reverse process of converting back the cipher text into original data known as ***Decryption***. Therefore, in order to hide the data or information from outsiders and to make it secure while transmitting, the concept of cryptography is used. Before discussing the encryption method, let us have a look on the types of cryptography techniques.

iii. Types of cryptography

Symmetric key cryptography (also known as secret key cryptography) and Asymmetric key cryptography (also known as public key cryptography) are the two cryptography method.

II. RELATED WORK

[Rashmi Rao et. al 2014] proposed improving security for data migration in cloud computing using encryption randomized technique. In this paper they proposed that with the development of the cloud computing the security of the data is becoming major concern of user. So accordingly no one trust third party for the safety of their data so they use1. the different techniques of data migration. Cloud computing have different paradigms in the world of computing resources. Collection of machine and resources and services2. forms a cloud in computing technology. In the cloud computing multiple resources and services are provided over the internet to the user. It is helpful to the user to reduce their3. operating and maintenance cost. In the cloud move the data4. from one to another target cloud which may be a public, private and hybrid cloud. It also require to maintain the need of organization with different models of Database as a service. In this process it face some issues like integrity, security, privacy, accuracy and others. In their proposed5. work they created an encryption algorithm which provides6. security to data.

III.METHODOLOGY

The designing of an encryption algorithm known as an "Enhanced encryption" method that makes use of both **public key encryption** and **private key encryption** in a combination along with the concept of randomization rather than using a single encryption technique (either public or private encryption), so as to find the better solution for the maintaining security.

IV.RESULTS AND DISCUSSION

In this research paper, we aimed at improving the security of data within the cloud when the data is migrated from one source to cloud or vice-versa, using an enhanced randomized encryption technique. Here for the experimental results, we would consider some useful data amount required for performing the enhanced encryption technique which are in the form of key size, data, time duration or message size to be encrypted and decrypted by using the proposed algorithm of encryption as discussed in this thesis. Therefore, the requirements for performing an experiment are as follows:

Data required for performing AES algorithm in the given research project are:

1. The random key size that has been generated by using a pseudo random generator : 32- bits
2. Message length or size of data to be encrypted : 32-bits or 16 bytes

Data required for performing RSA algorithm in the given research project are:

Key-pair: 1024- bits (for designing public key and private key of RSA algorithm)

Now, by taking all these data, an experiment will be performed to implement the enhanced randomized encryption technique within the cloud environment as follows:

Initially, a random key of 32-bits is used to encrypt the message or data of size equals to 32-bits using the symmetric AES encryption algorithm.

After encrypting the data of 32- bits, the random key of size 32-bits is then encrypted by recipient's public key using asymmetric RSA encryption technique.

Now, the encrypted data and the encrypted random key are then concatenated or combined together and are then stored in the cloud by the cloud service provider(CSP) such that when the user requests the encrypted result, then it will be delivered to the users/clients by the CSP.

Here, the user or client also is provided with a public key of RSA encryption algorithm by the CSP so as to store their data and hence this key is shared by both the users and the cloud service provider whereas the random key is used only once for encrypting the data and then can be removed or destroyed. In this experiment , when the user wants their encrypted data, then the CSP first checks for its authentication and then delivers the encrypted result to its real user.

Similarly, the decryption process will be carried out in which the ciphered random key will be decrypted first by RSA method using recipient's private key. Then this decrypted random key will be used further to decrypt the ciphered text using AES method.

In this way, this experiment aimed at providing confidentiality, integrity of data and authentication of the origin of data in a sense that the information or data should remain private while migrated, integrity of data so as to verify whether it has been attacked by an intruder or not and the authentication of the origin of the data as to know from where the data came. Also, there are more computations

involved in the proposed randomized encryption (hybrid) technique in comparison to AES or RSA singly. Hence, it has been concluded that it will take much time to encrypt the data as compared to the time taken by either AES or RSA alone and thus it will be very difficult for the cryptanalysis to break the randomized encryption (hybrid) technique.

V. CONCLUSION AND FUTURE SCOPE

It has been concluded that the enhanced (hybrid) randomized encryption technique can be used easily and efficiently for providing electronic security as compared to other traditional encryption techniques. The electronic communication involves the online banking, shopping on internet, e-mail system etc. which can be made strongly secured using the proposed enhanced randomized encryption technique. In future, we will try to focus on more security issues of cloud computing and give some better and some more practical implementations or solutions to achieve strong security using cryptography in data migration process.

VI. PROPOSED WORK

1. Enhanced Encryption Technique

The enhanced encryption technique used in our proposed work is basically a combination of public key (asymmetric key) encryption technique and private key (symmetric key) encryption technique. This encryption technique is said to be an enhanced encryption technique as it involves the merging of two or more encryption techniques such as a combination of asymmetric and symmetric encryption so as to take out the benefits from each of them is known as ***"Hybrid Encryption***" or "***Enhanced Encryption***".
This kind of encryption provides a high level of security to the encryption system because of the presence of highly secured public and private keys.

1.1. Concept of Randomization in encryption

The concept of randomization used in our enhanced encryption technique where plain text P is encrypted into a number of cipher texts and then randomly select any one of the N cipher texts and secondly, enciphered the plain text by mapping any of those cipher texts back into the original plain text since the one who decrypts the text has no knowledge about which one has been picked. Since the message space will increase in size by adding a random cipher text to it, the randomized encryption procedure will attain a high level of security in cryptographic systems and this system when used in cloud computing environment will provide a strong and more secured data migration process.

Therefore, by connecting a set of cipher texts or codes to each plain text or encoding a plain text by randomly selecting any cipher text from a set of cipher texts, the randomization in encryption enhances strong security to such codes or cipher texts against the attack on the given plain text.

The procedure of encryption using randomization can be defined by a relation 'A' which is a subset of (M*K*C). Here, 'M' refers to message space, 'K' refers to key space and 'C' refers to cipher text space. Now consider two cases as given below:

Case 1: At most one message x belongs to M (message space) for each key k belongs to K (key space) and each cipher text c belongs to C (cipher text space) such that (x, k, c) belongs to 'A'.

Case 2: In it, at least one cipher text c belongs to C (cipher text space), for each key k belongs to K (Key space) and each message x belongs to M (Message space) such that (x, k, c) belongs to 'A'.
Hence, the randomized encryption system can be defined as the quadruple (M, K, C, A).

From the above two cases of randomized encryption procedure, it has been concluded that the size of the cipher text space 'C' will be large as compared to size of the message space 'M'. This would further lead a transmitting channel to expand its bandwidth as the larger-sized cipher text space requires more bits to be transmitted for its identification rather than identifying the comparatively smaller-sized message space. Since the bandwidth is increased during randomization encryption, this is known as ***"Bandwidth Expansion".*** This is the only disappointing factor that cannot be avoided, while implementing the randomized encryption technique in the cloud environment and it causes a major cost in using such type of encryption.

Hence, considering as a useful solution to this problem, a factor for expanded bandwidth has been defined. This factor is calculated as the ratio of number of cipher text bits transmitted to the corresponding number of message bits as shown below:

$$\frac{\text{Number of transmitted cipher-text bits}}{\text{Number of corresponding message bits}}$$

Figure 1: Bandwidth Expansion Factor

Since the problem increased bandwidth cannot be discarded, but can be handled and controlled by the bandwidth expansion factor. Also if this factor comes to be variable then an average bandwidth expansion factor must be calculated instead of bandwidth expansion factor.

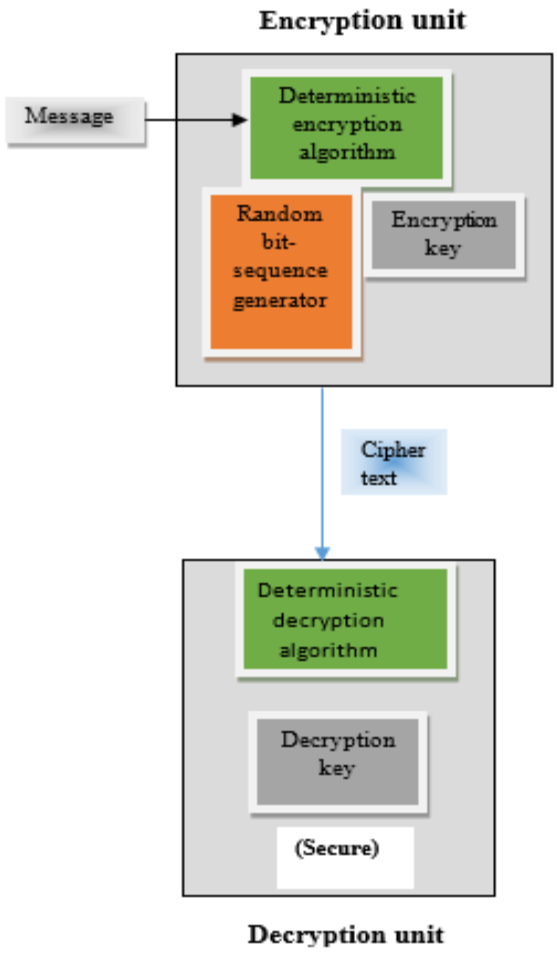

Figure 2. Randomized Encryption Procedure

The above diagram represents the transfer of data in a secure manner by the randomized encryption procedure over an insecure channel of communication and the random bit sequence generator is located inside the encryption unit in the secure area such that the enemy would be unaware about the output coming out of the random bit sequence generator. According to the concept of randomization within the block cipher, we will encrypt the given message in the following manner:

$$E_R (M) \parallel E'R$$

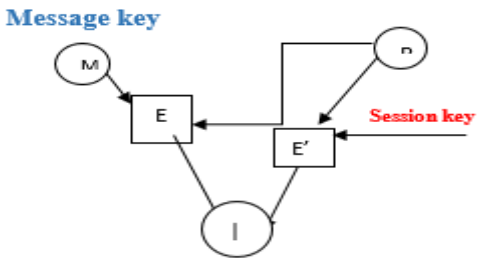

Figure 3: Proposed Encryption technique

In this technique, the message M is encrypted by a random key (message key) and that random key is also encrypted with a session key and then both results are concatenated. Its major advantage is that it minimizes the malicious or brute force attack on its encryption function and also leads to small bandwidth factor due to the longer length of message than random sequence.

1.2. Enhanced Randomized Encryption algorithm:

- ***For encrypting a message in randomized hybrid system:***

1. Initially generate a random key
2. Encrypt the data using that random key
3. Encrypt the random key with shared / session key
4. Forward both the data and key after encryption process from step 2 and step 3 together to the recipient.

- ***For decrypting the hybrid cipher text:***

1. Now decrypt the encrypted random key with the receiver's private key. Then, decrypt the encrypted data with the decrypted random key.
2.

ACKNOWLEDGMENT

I would like to express my sincere appreciation to Department of Computer Engineering & Information Technology, Suresh Gyan Vihar University. This study would not have been accomplished without their guidance. My sincerest gratitude goes to **Manish Sharma,** Head of Department of Computer Engineering & Information Technology Department, who guided me with his dedicated attention, expertise and knowledge throughout the process of his dissertation.

REFERENCES

[1] Secure Migration of Various Databases over A Cross Platform Environment, an International Journal of Engineering and Computer Science ISSN: 2319-7242 Volume 2 Issue 4 April, 2013.
[2] Understanding pricing and migration cost for Cloud adoption in business environments by Dimitris Monogenis, MSc Computing and Management 2011/2012.
[3] Mobile One Time Passwords and RC4 Encryption for Cloud Computing , Master's Thesis in Computer Network Engineering by Markus Johnsson & A.S.M Faruque Azam.
[4] 15th International Conference on Management *of* Data COMAD 2009, Mysore, India, December 9–12, 2009 ©Computer Society of India, 2009, A Unified and Scalable Data Migration Service for the Cloud Environments.
[5] Data Migration: Connecting Databases in the Cloud, a research paper published by authors: Farah Habib Chanchary and Samiul Islam in ICCIT 2012.
[6] Using the cloud for data migration: practical issues and legal implications - 16 Feb 2011 - Computing Feature.
[7] Database security in the cloud by Imal Sakhi, Examensarbete inom Datateknik Grundnivå, 15 hp Stockholm 2012.

[8] A Symmetric Key Cryptographic Algorithm by Ayushi, ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 15
[9] Microsoft Data Encryption Toolkit for Mobile PCs: Security Analysis **Version 1.0,** published: April 2007.
[10] "A Security approach for Data Migration in Cloud Computing", an International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013 1 ISSN 2250-3153.
[11] "Cloud computing a CRM Service Based on Separate Encryption and Decryption using Blowfish algorithm", International Journal on Recent and Innovation Trends in Computing and Communication Volume: 1 Issue: 4 217 – 223
[12] Slim Trabelsi, Yves Roudier. , Research Report RR-06-164 Enabling Secure Service Discovery with Attribute Based Encryption.
[13] RSA algorithm achievement with federal information processing signature for data protection in cloud computing, International Journal of Computers & Technology, ISSN: 2277-3061 Volume 3. No. 1, AUG, 2012.
[14] International Journal of Scientific Research in Computer Sciences and Engineering (ISSN: 2320-7639)
[15] International Journal of Scientific Research in Network Security and Communication (ISSN: 2321-3256)

Authors Profile

Akanksha Aasarmya pursued Bachelor of Engineering and Technology in Computer Science and Engineering from Suresh Gyan Vihar University, India in 2018. She is currently pursuing Master of Technology in Center of cloud infrastructure & security from Suresh Gyan Vihar University, her main research work focuses on improving security for data migration in cloud computing using randomization encryption technique.

Sohit Agarwal is an Assistant professor of Department of Computer Science and Engineering in Suresh Gyan Vihar University, India. He has done Master of Computer Application in Computer Science and Engineering. He has experience of 13 years in his field of Computer Science and Information Technology.

