IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 6 (May. - Jun. 2013), PP 39-42
www.iosrjournals.org

Improving security for data migration in cloud computing using randomized encryption technique

Rashmi Rao[1], Pawan Prakash [1]
[1](Dept .of Computer Science and Engineering, Gyan Vihar University, Jaipur, Rajasthan, India)

Abstract : *With the increase in the development of cloud computing environment, the security has become the major concern that has been raised more consistently in order to move data and applications to the cloud as individuals do not trust the third party cloud computing providers with their private and most sensitive data and information. In this paper, I proposed an encryption technique in cloud computing environment using randomization method to increase security and optimize the encrypted data in migration process.*

Keywords – *Attribute based encryption, cloud computing, data migration, prediction based encryption, randomization*

I. Introduction

Cloud computing has become the emerging paradigm in the world of computing resources [1] and is considered far better than the traditional paradigms of computing. The collection of machines and web services forms a cloud in cloud computing terminology. The various computing resources and applications are provided over the internet by cloud computing paradigm on the basis of different demands of its customers. Moreover, it also helps in reducing their operating costs and risks and thus presenting cost-effective solutions to various enterprises.

These numbers of benefits are the reason for organizations to bring the migration of resources and its applications into cloud. Data Migration is a turning point in the cloud environment that brings the new way to perform the risk management. It is a method to move or migrate the data, resources, applications or other beneficial components from any organization's on-site system into cloud or from one cloud to another cloud. The migration of the latter type is generally called as cloud-to-cloud migration. Along with its benefits, data migration in the cloud possesses some major security issues also such as data confidentiality, data integrity, reliability and portability of data and application, data security etc. Thus in this paper, we are proposing a modified and enhanced encryption algorithm with the concept of randomization in order to make the migration of data in the cloud more secure and optimized. This paper further proceeds with the following sections:

1. Cloud computing and its services
2. Data migration and its Security issues
3. Literature review
4. Proposed work
5. Conclusion
6. References

II. Cloud Computing And Its Services

Cloud computing is an emerging paradigm for computation of number of resources [1] and data than the traditional methods of computing. In other words, cloud computing is an advanced technology that brought up the concept of providing computing resources over the internet. It is the pool of resources and applications that are available to its users via internet and provides variety of computing infrastructures for various applications of processing data and its storage.

Cloud computing also describes – platform and type of application. By describing platform, it means to supply the machines or servers – whether a physical machine or a virtual machine and also to configure and reconfigure these machines.

On the demand of its users, the various computing resources are likely to be available over the internet through cloud computing. In this manner, different forms of resource –hardware and software resources can be utilized in a flexible and scalable manner thereby reducing their costs and providing cost-effective solutions to various enterprises. Therefore, cloud computing can be compared to e-business and it is considered as influential as e-business [1].

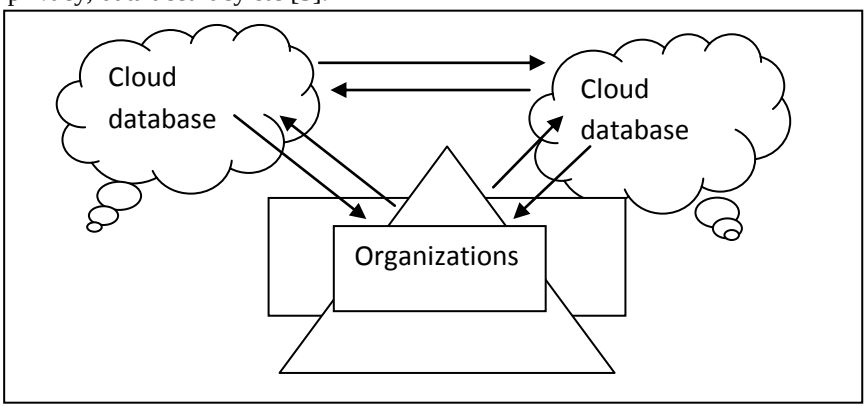
2.1 Cloud Services

There are three on-demand services classified by cloud as follows:

Software as a service (SaaS) in which application softwares are provided as a service to the clients via internet which are totally under the control of cloud service providers. It provides transparency of data.
Platform as a service (PaaS) in which platform or solution stack is provided as a service without operating the hardware and software layers and its cost and complexity.
Infrastructure as a service (IaaS) in which infrastructure or a virtualization environment is provided as a service.

III. Data Migration In Cloud

It is the method of moving a large amount of data and applications into the target cloud where the target cloud can be – a public, a private or hybrid cloud. [4] Since large numbers of applications are required to fulfill an organization's business needs and to improve its growth, various models of DaaS (Database as a service) are now provided keeping in view the data migration process. The data can be migrated in several ways such as –from any organization to a target cloud or from one cloud to another cloud.[3] But it is quite challenging task to migrate data and it involves various major security issues as well like data integrity, security, portability, data privacy, data accuracy etc [5].



3.1 Security Challenge In Data Migration

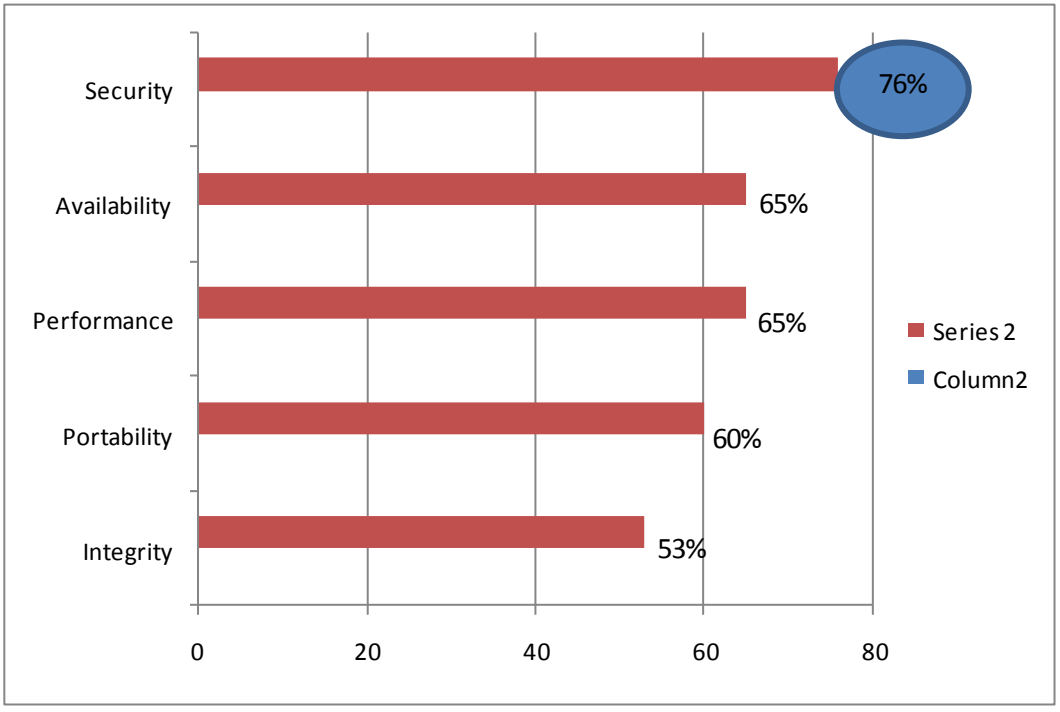


Fig2. Rate Chart of Major Issues in Cloud

Now, from the above rate chart of various issues in the cloud, we can see that the security is the major concern and hence, it is needed that the global security threats of the cloud should be prevented. Thus there is an ample need for securing data migration process and improving its security. In order to strongly secure the data

migration process, we tried to propose an improved and enhanced encryption algorithm by using the concept of randomization.

IV. Literature Review

As far as the security issue for data migration is concerned, the various cryptographic methods have been used earlier such as Identity Based Encryption (IBE), Attribute Based Encryption (ABE) and Prediction Based Encryption (PBE). [7]In Identity Based method, a unique identifier of the receiver such as e-mail address is used for calculating the public key by the third party servers. In contrast with typical public cryptography, this method proved to be more beneficial for reducing the complexity of processing the encryption method. But this method proved to be less effective for making the data more secure and optimized for migration as it needed a centralized server and secure channel between the source and destination.8] Then Sahai and Waters (2005) introduced the concept of attribute based encryption method, in which instead of using identifiers, an attribute was taken into consideration for encryption method. But it also proved to be weak for ensuring strong and secure data migration.

After these methods, a new method has come into consideration known as Prediction Based Encryption (PBE). [6] This method is generally used for multicasting and is originated from both –Identity Based Encryption (IBE) and Attribute Based Encryption (ABE). While in IBE method, identity of an entity is used for encryption key and decryption key as well, the PBE (prediction based encryption) method is much better scheme as the identity of an entity is derived from a set of attributes and for decryption, access policies are there. [3]

It includes following four steps for performing encryption, decryption and generating key.

a) SetUp: to generate a secret key that acts as a master key, for generating decryption key and a set of public parameters.
b) KeyGen: a decryption key is generated by using this operation.
c) Encrypt: this operation performs the encryption of plain text with the help of public parameters and supplied encryption key.
d) Decrypt: is used for decrypting the cipher text.

In this way, Prediction Based Encryption method proved to be effective for providing security of data in cloud. But, still it lacks a more efficient mechanism for making data security stronger and maintaining the work reliability. Therefore, in this paper we proposed an approach of using randomization and creating an enhanced encryption method so as to improve the security of data migration process in cloud.

V. Proposed Work

In my proposed work, I am creating an encryption algorithm to provide strong security to data in cloud that would be better in performance than using already existing encryption algorithm like PBE(prediction based encryption),IBE(Identity Based Encryption) etc.

In this encryption method, the concept of randomization will be used. In randomization concept, we initially start with encrypting a single plaintext P into a number of cipher texts such as $C_1, C_2, \ldots C_n$ and then randomly select any one of the N cipher texts and secondly, map 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.

One thing that must be taken into consideration is that the cipher text should be longer in length as compared to the plain text otherwise a problem may occur. It means that the cipher text should be atleast $\log_n$ bits longer so as to perform better. In this way, $n2k=2k+\log_n$ cipher texts are there and $2k+\log_n$ bit pattern will be available to express them.

5.1 Enhanced algorithm is as follows:

For Encryption

1) Initially, generate a random key.
2) Encrypt the data using that random key.
3) Encrypt the random key with the shared key.
4) Forward the data after encryption process from step 2 and step 3 together.

For Decryption

1) Now decrypt the encrypted random key with the shared key.
2) Then, decrypt the encrypted data with the decrypted random key.

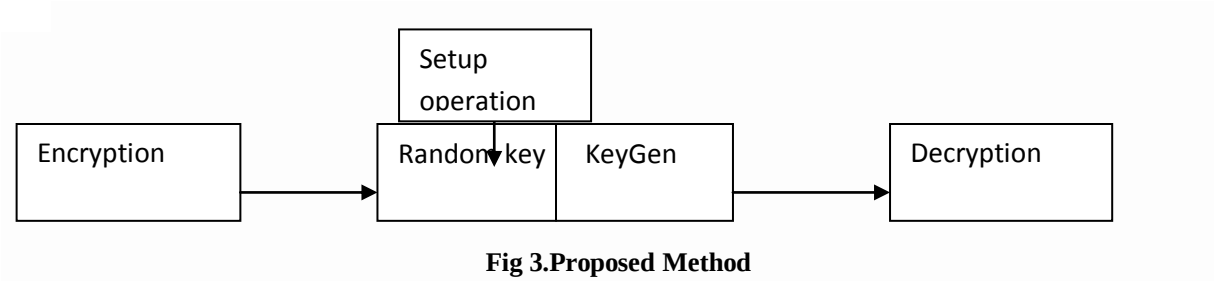


Fig 3.Proposed Method

Here, the shared key is re-used but the random key is used only once for encrypting data. Hence, by applying this method, the data can be made more secure and reliable as the outsider will have no idea about what data is encrypted with the persistent key.

VI. Conclusion

Since the security challenges are increasing day-by-day in the cloud computing environment and the privacy of clients is at risk as the data is transferred from one cloud to another cloud during the migration process. The security of data has become the major issue in cloud environment. Here we focused in improving the data security with the randomized encryption technique.

After proposing this enhanced encryption algorithm using randomization technique, we came to the conclusion that by creating a random key for encrypting the data, the attacker can get confused over what data is encrypted with persistent key and he becomes unable to analyze even by comparison that if the two encrypted texts corresponds to the same plaintext. It means that if an outsider or attacker encrypts the plaintext or obstructs the cipher text, then he can simply compare among the encrypted message. But the advantage of adding randomness is that the risk of attack from the unknown outsider can be easily removed. In future, we will try to focus on more security issues of cloud computing and give some better solutions to achieve strong security using cryptography in data migration process.

References

[1] 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
[2] Gartner (2008). Gartner Says Cloud Computing Will Be as Influential As E-business. Gartner press release, 26 June 2008. http://www.gartner.com/it/page.jsp?id=707508. Retrieved 3rd May 2010.
[3] Secure Migration of Various Database over A Cross Platform Environment, an International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 4 April, 2013
[4] Data Migration: Connecting Databases in the Cloud, a research paper published by authors: Farah Habib Chanchary and Samiul Islam in ICCIT 2012.
[5] Using the cloud for data migration: practical issues and legal implications - 16 Feb 2011 - Computing Feature
[6] 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
[7] QuickStudy: Identity-based encryption by Russell Kay
[8] Research Report RR-06-164 Enabling Secure Service Discovery with Attribute Based Encryption, by Slim Trabelsi, Yves Roudier.