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

[1]Akanksha Aasarmya , [2]Sohit Agarwal
[1]Research Scholar, [2]Assistant professor
akanksha23995@gmail.com , sohit.agarwal@mygyanvihar.com
Center for cloud infrastructure and security
Suresh Gyan Vihar University, Jaipur

Abstract: The data-center 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.

Keyword: -*Data Migration, Cloud Service, Security, data Transfer.*

1. Cloud Computing :

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. It is a technique in which we have the access to our data and application globally, from each and every part of the world having an internet access. The data and applications are situated remotely over the central remote server. In other words, it is the methodology of delivering the services online. With Cloud Computing, we can cut the operational and capital costs and can focus on the respective project instead of keeping eye on the functioning of the datacenter. For example, remember the times when we installed Microsoft office on each of our organization's computers. Either we go around with a setup disc to install it on all the machines or we had a setup of our software distribution servers to install the application on the machines. And when there is a service pack issued by Microsoft, we again have to run around and install the pack or we have to re-setup our software distribution servers to distribute it accordingly. The license involved is very costly. We may use the office applications only a few times a week, but the cost of the license is same as everyone else's. The main advantage of cloud computing technology is that some other company is hosting our application i.e., they handle all the cost involved for the servers, manage the software updates and modifications, and the pay-per-use policy authenticity. 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. These services themselves are being referred to as Software as a Service (SaaS).

Data center hardware and software, combined, we are referred to as a cloud. When it is made available to the general public in a cloud-in-the-go system, we call it as a universal cloud. The services sold here are called utility computing. Current examples of public utility computing include Amazon Web Services, Google App Engine and Microsoft AZURA. The private cloud is used to refer to the internal data centers

of a business or other private organization that is not open to the public openly. We will usually use cloud computing, it will only replace transparency with other terms when it claims transparency.

Service providers greatly simplify and enjoy software installation and maintenance and facilitate central control over different versions; End users can access the service "anytime, anywhere", share information and collaborate more easily and can safely store their data in the infrastructure. Cloud computing does not change these things, but it gives more applications and service providers the freedom to supply their products without providing data center as a service: such as the rise of semiconductor foundries, chips allow companies to design and sell chips. Owned by a fable. From now on we will focus on possible issues related to SaaS Providers (cloud users) and cloud providers, which receive less attention.

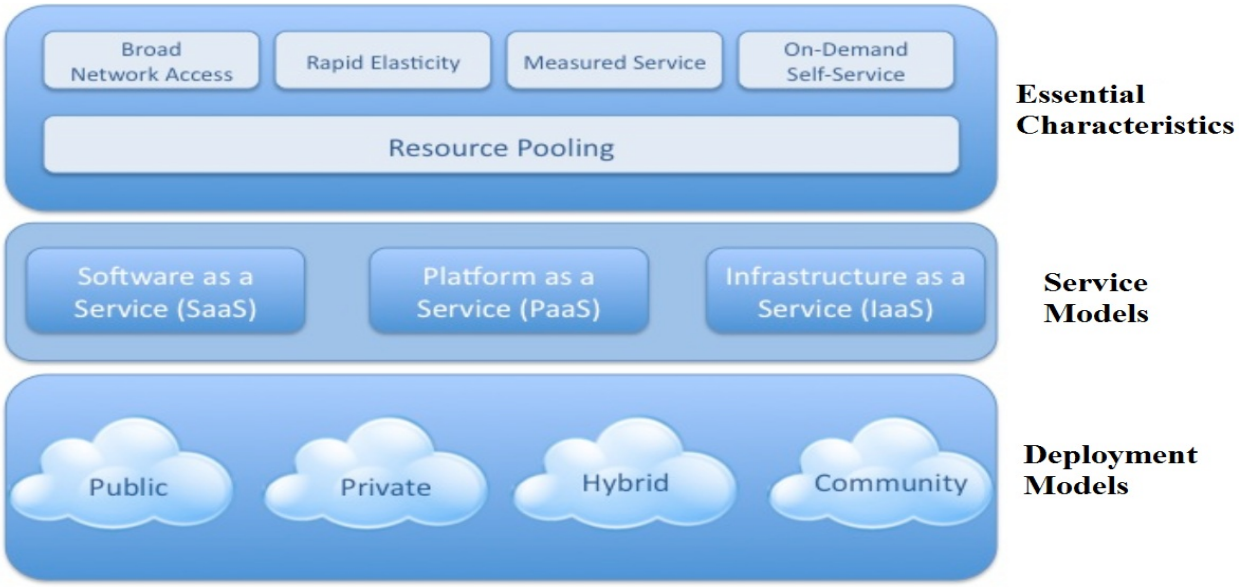

Fig.1.1. Cloud Computing Model

1.1.Essentials characteristics of cloud computing

I. **Broad network access: A** broad network is provided by the cloud that offers various capabilities to be accessible via different standard mechanisms.
II. **Rapid elasticity: It** means that the rapid and elastic capabilities are provided within the cloud and are unlimited.
III. **Measured service: It** involves monitoring, controlling, optimizing and reporting of resource usage in the cloud systems so as to provide some transparency for its customers and service providers.
IV. **On-demand service: It** describes the feature of offering on-demand self-service to the customers without interacting with service provider.
V. **Resource pooling:** It refers to the pool of resources that are made available over the cloud to number of consumers by using multi-tenant cloud model. These resources can be either physical or virtual resources that are assigned according to customer's needs

1.2 **Cloud Service Models:**

I. **Software as a service (SaaS):** It provides transparency of data and is considered as the top-most layer of the cloud. This service provides such applications which provide an API – responsible for extending bigger and large number of applications for example, Google Docs. The clients are provided with hardware infrastructures service and software products as service either on demand in" pay-as-you-go" model or without any charge. Thus , SaaS has made a renowned position in the market of business including tasks such as web-based e-mail, database processing, ERP software, content management, accounting software, customer relationship management(CRM) etc [2,3].

II. **Platform as a service (PaaS):** The task of writing, deploying or managing the various cloud applications are performed over the platform provided by PaaS. Moreover, it is useful in offering various development tools as well as administration and management tools, security services, run-time and data management engines. Force.com, GoogleApps and Amazon Web Services are all examples of PaaS [2, 3].

III. **Infrastructure as a service (IaaS):** In this service, the highly scalable and elastic computing infrastructure such as virtual servers, storage, databases etc are available for users so as to run the applications. The IaaS includes examples such as: elastic compute cloud of Amazon, a web service platform and Eucalyptus, an open source platform [2].

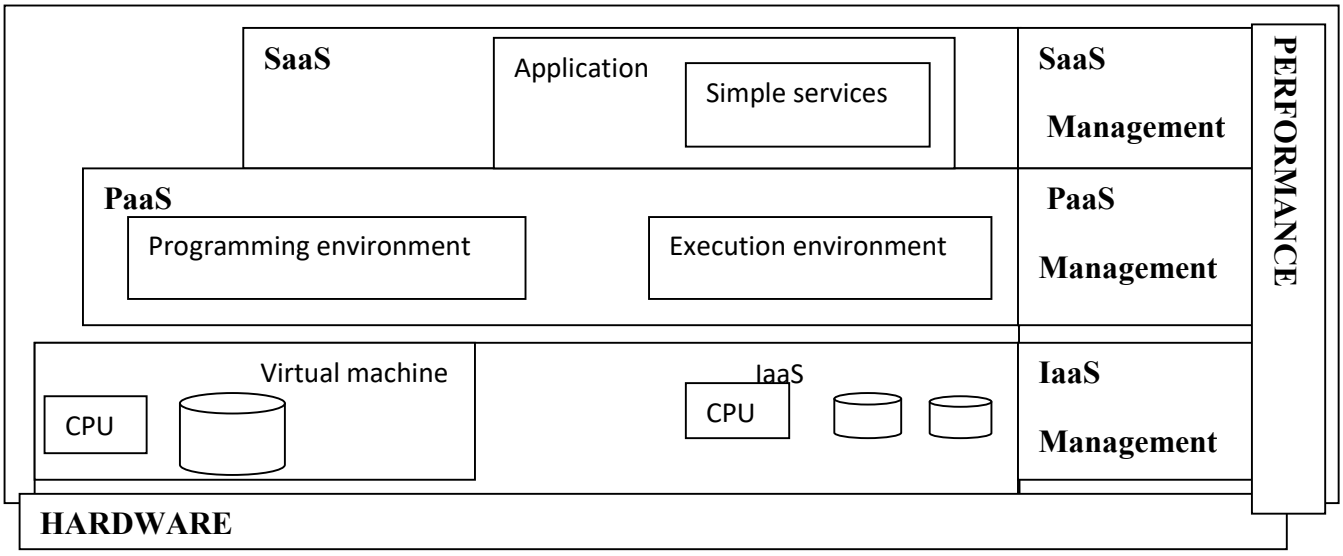

Fig.1.2 Services of Cloud

13. C**loud Deployment Models**: The cloud deployment models are classified into following four different categories [2, 3]:

Public Cloud: A public cloud is the type of deployment model which is publicly available for sharing and is accessible by all the users over the internet. In this model, the services in the form of applications and resources are delivered to general public via internet or web services. Moreover, it is quite simple and inexpensive set-up as the services offered through this type of model are either freely available or on a "pay-as-you-go" model and its bandwidth and application costs are handled by the service provider. Some examples of public cloud are: Google AppEngine, IBM's Blue cloud, Sun cloud etc. [2, 3].

Private Cloud: A private cloud is the type of deployment model which is privately available to the users. They are privately owned and provide private services to limited number of users so as to reduce the security risk. Since it is the corporate firewall in which the private cloud is implemented, it is also known as the "corporate cloud" or "internal cloud". Though the private cloud possesses the features and benefits similar to the public cloud, the major advantage of designing a private cloud lies in removing the various numbers of objections that occurs in the cloud computing environment such as control over the customer and enterprise data, security risks etc. Some examples of private cloud are: Amazon's Elastic Compute Cloud (EC2), Simple Storage Service (S3).

Hybrid Cloud: A hybrid cloud is the type of deployment model which provides the combination of services in the private manner as well as in the public manner such that infrastructure is partially hosted inside the organization and externally in the public cloud. In it, the private cloud delivers the core services and the public cloud give rise to other services. For example, Amazon Simple Storage Service (Amazon S3) acts as a public cloud service for recording data of the organization and also as the private cloud service by providing in-house storage of customer's operational data.

1.4Data migration in cloud computing

The object of an organization can be moved from the cloud to cloud or data from one cloud to another. [4] 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. [6] to achieve an automatic data migration, a programmatic data migration approach is required to get rid of the tedious tasks of a human organization.

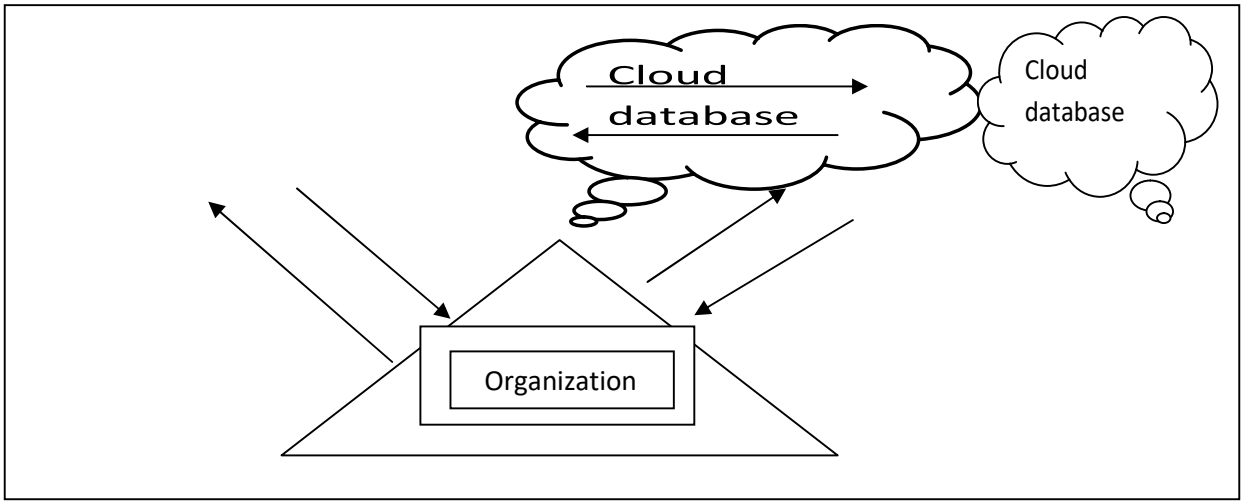

Fig.1.4. Data Migration in Cloud

1.6 Need for migrating data into the cloud

For integrating data under the various projects of the enterprise, data migration plays a key role in the field of cloud computing technology. Since business demands are growing rapidly so more and more applications are required to support these demands and for this purpose, the cost involved for running and managing the databases for applications are affecting badly due to the emerging demands. Therefore, in order to gain the benefits of cloud computing and to meet the growing demands by resolving the cost issues for integrating data for any organization, there is much need for bringing the concept of data

migration into the cloud. And for this reason, cloud computing has brought its new service model as the data migration as a service (DMaaS) model.

In the simplified form, the need for migrating data into the cloud arises if merging of the computer systems is performed or is the old computer system is to be replaced by the new computer system or is upgraded to new system by the organizations. All above reasons supporting the need for data migration in the cloud are summarized below:

a) If a company wants to transfer its data to another company in a thought to get better support for their requirements by another CSP.
b) To gain the benefits of emerging cloud computing paradigm for meeting growing business demands.
c) When the systems or accounts are to be merged by an organization after acquisition

2. Literature Review

[Tamanna Narula et. Al 2014] proposed framework for analyzing and testing cloud based application. In this paper they proposed that software testing is the main processing of accessing functionality and correctness off a program through analysis. In software engineering related projects testing has become the challenge, especially for the major system. Because testing can be such a difficult and costly and more manpower required process. [4]

[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. [5] In the cloud move the data 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, [5] accuracy and others. In their proposed work they created an encryption algorithm which provides security to data.

[Nirav Shah Et. al 2015] proposed secure data migration in cloud providing integrity and confidentiality. Cloud computing is a new feature which adds many features and application together on a platform over internet for better IT infrastructure and cost effective organization. The security has been become major issue n term of moving data of user from one machine or a server to another in the development of cloud computing.[6]. In their proposed work they created an encryption algorithm to secure the data in cloud which gives better performance and better results more than the already existing algorithm like PBE and IBE. [1] And they conclude that cloud computing is increasing the business with high usage of data and it is helpful for the companies and other who are using the cloud services. By providing the encryption, confidentiality, integrity data can be more secure and security of data is the priority of everyone.

[Dhrumil Parikh et. al 2015] have proposed migrating algorithm for data security in cloud computing. In this paper they described IT firms are converted their self into the cloud based infrastructure through internet resources. And security is becoming the major concern of the companies. Transmission of data called migration which can be online or offline. Cloud computing is defined as set of resources and offered service. It conveys everything as a service over the internet based on demand of user.

[Shyamli Dewan et. al 2015] proposed that cloud computing has become a future generation infrastructure for computing. Normally cloud computing is defined as a bunch of computing resources access by internet. [8] Basically user store their data in the cloud with firewall and other security to keep the data safe from third party or some intruders. In the cloud computing resources there are many service providers who provide the services to the user and it's their duty to keep the data safe of the user or

protect the data from unwanted access or the user can take the help from the Third party auditor to keep their data safe from the unwanted access and provide the security to their data in cloud over the internet.

[Suganya .N et. al 2015] proposed implementing RSA algorithm to get the data security in cloud computing. Cloud computing is an internet based technology where a good amount of resources which is shared as a services. It is a payment based model where user pay money for the cloud services. Many organizations are afraid to store their data over the internet due to negative effects of cloud. With the help of cloud computing user can access the data and application from anywhere in the world with user authentication. And many user can access the same data in cloud system. [9] In their related work they mostly works in security of users data. In third party auditor and auditing mechanism are proposed.

[Shyamli Dewan et. al 2015] proposed secure data migration across cloud system using TPA. Cloud computing is acquiring as future generation architecture of computing. Basically cloud computing is defined as a bunching of computing resources which is easily accessible via internet. Accordingly the user store their data in cloud with firewall and other security protection to make save their data from unwanted access and intruders to access the data. [10]

[G. Gowri Et. Al 2014] proposed cloud computing application and their testing methodology. In this paper they proposed cloud computing provides new security to the user. These new technology create a platform for the user of the opportunity and activate the internal operation of the cloud to the user. For provide the better quality of service it representing security testing and assure the better quality and accuracy for whatever user design. [11]

3.1. 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 enhancement of one encryption method by adding another encryption method so as to improve and thereby increasing the security strength while migrating data in the cloud computing environment. In other words, a way of encryption which 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.

To carry out this type of encryption, initially the symmetric or private key encryption is performed with the help of some unique keys which are randomly generated in order to transfer the data. After that, the randomly generated key is encrypted using the asymmetric or public-key by implementing the asymmetric encryption technique. Also, this public key of the recipient is then further used to decrypt the session key (random key) and at last, the data is decrypted by using the decrypted session key. In this way, by implementing an enhanced encryption technique in data migration process, a high level of security can be easily achieved.

Need for enhanced encryption technique

a) With the advent of cloud computing technology and the use of internet, security has become the major concern in cloud computing environment while transmitting data over the internet.
b) This is because the transmission of useful or sensitive data over the internet is quite unsafe and lacks trust.
c) Also, the increased versatility of the attacks over the internet cannot be handled completely by traditional single encryption methods.

d) Hence, this is the reason to propose an enhanced (hybrid) encryption technique by creating an enhanced encryption algorithm for improving data security during migration in cloud computing.

3.2. Concept Of Randomization in encryption

The concept of randomization used in our enhanced encryption technique generally defines a procedure in which initially a message or plain text P is encrypted into a number of cipher texts such as C_1, C_2,....., Cnand 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. Jefferson-Bazeries Wheel Cipher and its variations were used at the time of both world wars [Kru81] and [Kah67] by the U.S. is the best example of using the concept of randomization in encryption technique.

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:

$$\text{Bandwidth Expansion Factor} = \frac{\text{no. of transmitted cipher-text bits}}{\text{no. of corresponding message bits}}$$

Since the problem of expanded or increased bandwidth cannot be avoided or 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.

On the other hand, in a randomized encryption technique, the main focus is on generating random bits of data. Therefore, some source is required for generating such type of bits. There are various ways that can be used to create such source of random bits and the examples include –neon discharge tube, noisy diodes, radio-active decay or some other natural source for providing degree of randomization.
To define the generator, a relation is used known as the recurrence relation. This relation is shown as below:

$X_{n+1} = (pX_n + q) \pmod z$

Where, Xrepresents the pseudorandom sequence values, and the following constants define the generator as:

z, $0 < m$ is the modulus

p, $0 < p < z$ is the multiplier

q, $0 < q < z$ is the increment

X_o, $0 < X_o < z$ is the seed or salt value

Now, z defines the limit of a period in general LCG(Linear Congruential Generator) which means that the LCG generator have periods up to z and even less than this value for some p choices. Moreover, for the full period of LCG having q as non-zero, there are some conditions:

1. q And z should be relatively prime.
2. p-1 is divisible by all the prime factors of z
3. Also, p-1 should be a multiple of 4 if z is a multiple of 4.

By using the LCG pseudorandom sequence generator, a large number of random numbers will be generated and then be used to create a random key. Since a key of variable size is required for encrypting the random key that has been generated by a pseudo random sequence generator in our proposed randomized encryption technique, we now generate a key-pair out of a large number of size Z such that this large number is considered as a modulus for the public and private key and is then calculated by multiplying the two different prime numbers namely, x and y, i.e., Z= x*y. now the Euler's totient function is calculated as O(Z) = (x-1)(y-1). After the totient function is computed, now select an integer say p, such that it lies in the range of [1, O(Z)] i.e., $1< p < O(Z)$, and also p and O(Z) have only One as a common factor. Here, the exponent of public key is p. after defining the public key exponent then the exponent of private key is defined for satisfying the congruency q*p= 1 mod O(Z). In this way, the public key is obtained as: (Z, p) and private key is obtained as: (Z, q) nd all these values must be kept secret.

Conclusion:-

Encryption 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. Moreover, 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.

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. Understanding pricing and migration cost for Cloud adoption in business environmentsby 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. 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.
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 AnalysisVersion 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. Quick Study: Identity-based encryption by Russell Kay Slim Trabelsi, Yves Roudier. , Research Report RR-06-164 Enabling Secure Service Discovery with Attribute Based Encryption,