ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

Secure Data Migration across Cloud System Using Third Party Auditor (TPA)

Shyamli Dewan [1], Devendra Kumar [2], Sandeep Gonnade [3]

M.Tech. Scholar, School of Engineering & IT, MATS University, Raipur, Chhattisgarh, India [1]

M.Tech, School of Engineering & IT, MATS University, Raipur, Chhattisgarh, India [2]

Asst. Prof., School of Engineering & IT, MATS University, Raipur, Chhattisgarh, India [3]

ABSTRACT: Cloud Computing is evolving as future generation architecture for computing. Usually cloud computing is defined as a grouping of computing recourses accessible via internet services. Traditionally the client/user store data in data centres with firewall and other security techniques used to protect data against intrudes to access the data. The client/user has less control over the stored data on the cloud, since the data is stored anywhere across the globe. It is the responsibility of cloud service providers to protect the client/user data from unauthorized access & disclosure and be faithful for the development of cloud computing. A third party auditor (TPA) can be used to provide security services over the cloud and ensures client/user that his/her data is secure from unwanted and suspicious activity. The TPA would not store any kind of data at its end, and it is only confined to providing security service between cloud service provider and the user. During migration of data from one cloud to other cloud, the application framework will provide data integrity verification by using hashing algorithm like SHA-1 and provide encryption/decryption using symmetric algorithm like AES. We have proposed a secure mechanism to secure data migration between clouds using third party auditor (TPA).The proposed approach adapts the secure socket layer (SSL) protocol to increase the level of trust and security for both user and cloud service provider. Network simulation tool (NS-2) is used to analyze the fairness of the channel during data migration between clouds in terms of block encryption/decryption time duration. Our proposed mechanism improves the time constraint parameter for migrating data from one cloud to other.

KEYWORDS: Cloud computing; data migration; data protection and integrity, TPA.

I. INTRODUCTION

Cloud Computing: Cloud computing is a new kind of computing, which uses advanced computational power and improved storage capabilities. Cloud computing enables the sharing of services over the internet, which can be seen as a long dreamed vision of computing utility. We store information and run application at the Cloud, consists of a large group of interconnected computers. Cost savings is the main advantage over the cloud on the other hand its security is leading disadvantage. Many software industries use cloud computing like Amazon, Google,e-Bay and Facebook etc. Many companies adopt their own security structure because the security is not provided in cloud. Security is not guaranteed over the cloud since the data placed at cloud is accessible to everyone. Toensure security, cryptographic techniques cannot be directly adopted. On some occasion it is seen that the cloud service provider may hide the data corruptions to maintain their reputation, name and status. To avoid this kind of problem, we have introduced an effective third party auditor (TPA) to audit the user's outsourced data when required. The proposed approach adapts the secure socket layer (ssl) protocol to increase the level of trust and security for both user and cloud service provider.

Data Migration in Cloud: Data Migration is a process which involves moving a large amount of data or applications to the target cloud. The target cloud can be a public cloud, a private cloud or hybrid cloud. An organization's business needs large numbers of applications to fulfill and to improve its growth, now data migration process is provided as DaaS (Database as a service). The data can be migrated in several ways such as –from any organization to a target cloud or from one cloud to another cloud. Although it is relatively tough task to migrate data and data

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

migration involves various major security issues such as data integrity, confidentiality, security, portability, data privacy, data accuracy etc.[2][3][4]

i. ***Pre-Migration:*** In pre-migration scheme before migrating the data to cloud ,some transformational activities are done previously. These activities include server virtualization, server platform upgrades or data separation. The foremost purpose of this scheme is to make transformation easier by changing data into required format. So main advantage of this scheme is that it makes the migration process easier, faster or less risky.

ii. ***Post-Migration:*** In this method, transformational activity is done after the migration has completed to the cloud. Once the migration services have been successfully transitioned to the cloud, Data Centre Migration programmed should wind-down.

Third party Auditor (TPA): Third Party Auditor is kind of supervisor. There are two categories of TPA: private TPA and public TPA. Although, private TPA can achieve higher scheme efficiency than the public TPA. Public TPA allows anyone, not just the client (data owner), [12] to challenge the cloud server for the correctness of data storage while keeping no private information. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. To let off the burden of management of data of the data owner, TPA will audit the data of client. The released audit report will be beneficial to the cloud service provider to improve their cloud based service platform and would also help owners to evaluate the risk of their subscribed cloud data services. Thus TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner.
Security as well as data storage correctness is primary concern since cloud consumers save their data in cloud server. A new secure mechanism is introduced to provide security to different cloud types. The Secure Socket Layer (SSL) protocol is implemented to achieve data storage security. SSL protocol is efficient and safer than the other former secured algorithms.

II. RELATED WORK

Ateniese et.al (2007) [1] proposed a framework named as Provable Data Possession (PDP).In this PDP protocol is used which verifies outsourced data storage site retains a file which consist n blocks. With PDP, client first process the file named as F and add some data and expands it to a new file F'. After that client add some VMd (Verification metadata) named as M for file F' and stored it on cloud server. Generated M will also store on client local storage with metadata M. Client deleted metadata but before deletion client will execute a data possession to server by giving challenge to server to make sure that server successfully retained the file Yes or No response from server verifies the existence of file at cloud storage. In this Provable Data Possession system client issue a challenge and a send request(R) to compute proof of possession P and sends to client to verify results of integrity.

Cong Wang et al.(2010)[2] proposed an improved scheme of verify data integrity privacy preservation of data at cloud using concept of Third Party Auditor(TPA), since cloud user doesn't have expertise on auditing process so that client resort a TPA to audit data.[1][2][3][4]TPA audit data on behalf of user and check data integrity, confidentiality and privacy of data at cloud storage. [1][2][3][4] In this technique TPA enables to divide file (F) into n number of blocks and send to client. Suppose file is denoted by F and sequenced into N number of Block by M1, M2……Mi…..Mn using following function.

$$K*(0,1)* \longrightarrow (0,1)$$

In this model cloud user generate public key, private key and VMd to server. TPA verifies each blocks of file and recovers it if it is malicious.
Venktesh. M. et al(2012) [3]also provided a similar solution to Cong Wand et al TPA model, but they added RSA (Rivest, Shamir, Adelman) algorithm for security and integrity of data storage. In this proposed scheme client generates signature for each block of file with secret key using RSA and a Hashing Algorithm

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

$$Ti= h(Mi).gMi.rsk$$

$$Ø= \{Ti\}$$

Where Ø is signature for all blocks.
They used Merklee hash Tree (MHT) is constructed by using all blocks, this tree is signed root by client with secret key

$$Sigrsk\ (H\ (R)=H\ (R\ )\ .rsk$$

In next step client sends file [1][2][3][4] hash and signed root (F, Ø, sigrsk HR)),during Audit process client through a challenge to server by selecting specific block. Server sends proof back to client. Clients verify it using MHT and secret key .
Sarfaj Nawaj Brohi et al(2013) [4] proposed recent technique using Trusted Third Party Auditing (TTPA)which contains five concepts RBAC(Resilient Role Base Access Control),partial homomorphic cryptography, metadata generation and sound stenography, efficient Third Party Auditing(TPA) and backup and recovery process. In this scheme they encrypts data storage file using public key and secret code. Encrypted file sends to cloud server, data inside file will be homomarphically encrypted and stored. Whenever client needs, it is decrypted using private key. After storing file cloud server breaks file into number of blocks and generate Verification Metadata (VMd). Client admin downloads and store VMd at its local storage and request cloud server to encrypt file, public key, private key and VMd using sound stenography. In sound stenography sound-1 contains public key and VMd and sound-2 contains private key. [1][2][3][4] Now TTPA download all these parameters to local storage and processed auditing process using fresh metadata and stored metadata, Based on results TTPA sends report to cloud server if data is malicious it request server to recover it.

III. PROPOSED RESEARCH MEHODOLOGY

In this research paper, the third party auditor (TPA) is used having a SSL protocol framework associated with user and cloud service provider. It will be fully automated and will be able to properly monitor confidentiality and integrity of the data. It uniquely integrate with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage while keeping all above requirements in mind. The simulation work is carried out with network simulation tool NS-2.We have implemented the ssl protocol to secure data migration between clouds effectively associated with the TPA. The performance analysis shows the proposed schemes are provably secure and highly efficient. Transmission of data will be encrypted; there is no corresponding key to be restored, even if the data is stolen. Simply the user distinguish the key, the clouds do not distinguish the key. Due to the properties of encryption, the cloud can operate on cipher text, and thus avoiding the encrypted data to the traditional efficiency of operation. The privacy of the USER is protected because user's files are encrypted in cloud storage . Our experimental results validate the effectiveness of our approaches and also show that our system has a lower computation cost, as well as lower time constraint integrity verification. Advantages of proposed approach are:

- In this paper a fragmental TPA mechanism is introduced with ssl protocol framework to improve performance and reduce extra storage.
- A TPA needs simply access file to perform audit in each activity and the audit activities are efficiently scheduled in an audit period. This reduces the time constraint in file (blocks) encryption/decryption phase during migrating data from one cloud to other.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

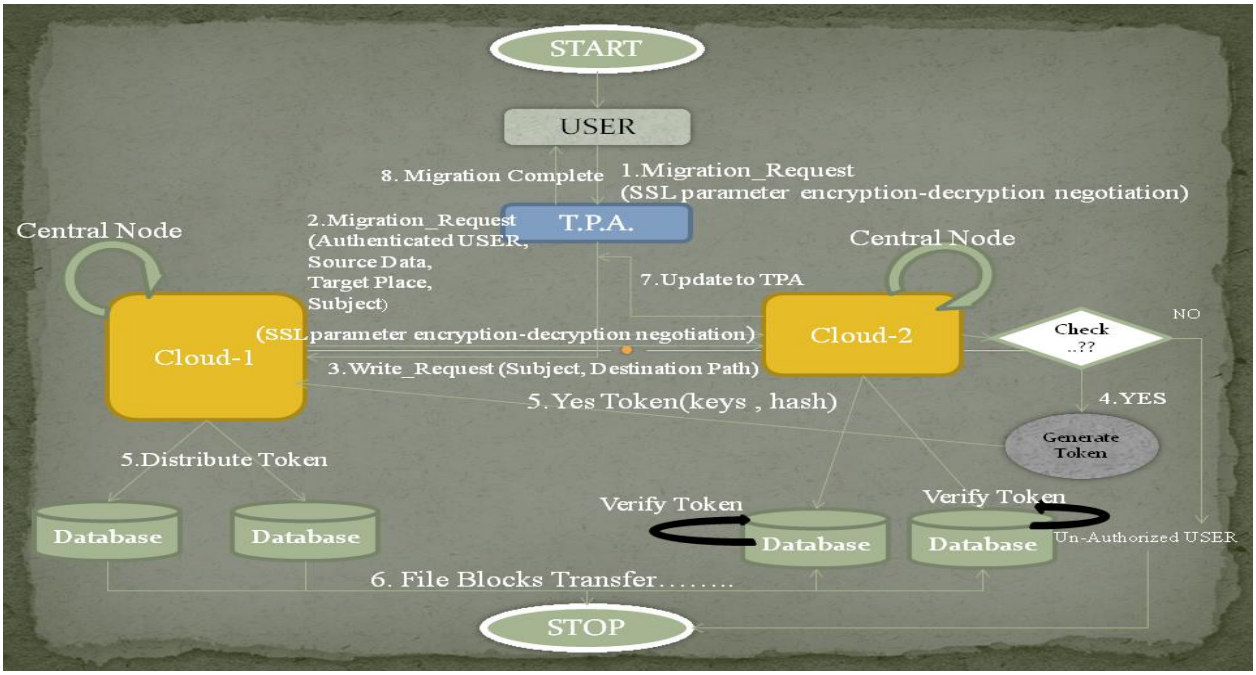

Fig.1: Proposed Research Methodology

In this paper, we consider data storage and sharing services in the cloud with three entities: USER, Third Party Auditor (TPA), and Cloud (shown in Fig. 1). As shown in Fig.1 [1][2]User is the original owner of data, and shares data in the cloud with other users. Other users in the group are able to access, download and modify shared data. [1][2]The cloud provides data storage and sharing services for users, and has sufficient storage space. [1][2]The third party auditor is able to verify the integrity of shared data based on requests from users, without downloading the entire data.
There are following steps for the whole migration process:

1. USER sends a migration request to the TPA. This negotiation is done under SSL protocol framework, just to ensure security.
2. After receiving the migration request, the TPA generates an auditing message to the cloud, and retrieves an auditing proof of shared data from the cloud.
3. TPA forwards migration request to the central node of cloud 1 including (Authenticated user, source data, target place, subject etc.). This negotiation is also done under SSL protocol framework, just to ensure security.
4. The central node of cloud1 sends a write request (subject, destination path) to central node of cloud2.
5. The central node of cloud2 checks the permission of USER to see if USER has enough right to write data to the specified path in the write request.
6. If the permission check succeeds, central node of cloud2 will synchronize with its data nodes to generate a write token (keys and hash) and send it to the central node of cloud1.
7. The central node of cloud1 distributes these tokens to its data nodes which stores the data that will be migrated.
8. The data nodes of cloud 1 send data and token to the target central node described in the token.
9. The central node of cloud2 verifies the token to see if the block can be written.
10. If the verification succeeds, the central node sends address of target data node to the source data node.
11. The source data node sends blocks to the target data node. This completes the migration of data from cloud 1 to another cloud2.

Thus, in proposed method, we take into account how to migrate data concurrently to decrease the time constraint over the cloud.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

IV. SIMULATION AND RESULT EVALUATION

Network Simulator tool NS-2 is used to evaluate the performance of our proposed work over the cloud. The SSL protocol is implemented in network and consequently effectiveness of ssl protocol is tested under TPA and cloud MDM modules .The performance is analyzed on behalf of metrics like block encryption and decryption phase.
The scenario design of simulation topology of cloud environment with TPA module and MDM module is shown in Figure 2&3.

As shown in Fig.2 the TPA module consists of two clouds with central node1 and central node2 respectively. These two central nodes are responsible to give permission to their data nodes to migrate the data among them.
USER initiates the migration request with TPA.TPA forwards the migration requests to the source cloud 1 and cloud2 via central nodes. After establishing secure connection through SSL protocol the migration process proceeds as described in migration process in section III.

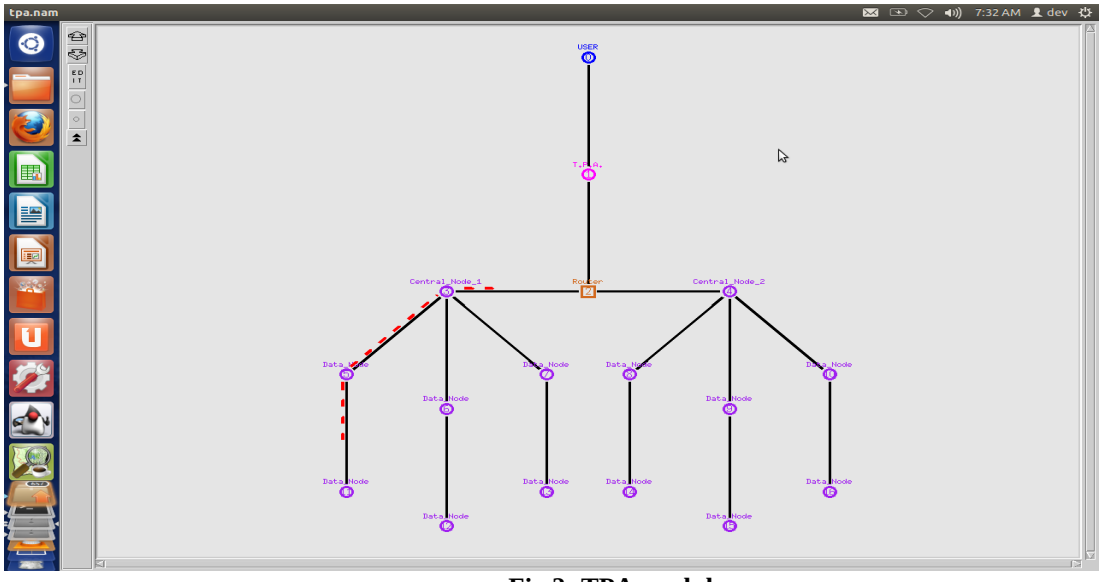

Fig.2: TPA module

Following Fig. 3 shows the MDM Module. The MDM module is implemented with two clouds with central node1 and central node2 without TPA (Third Party Auditor). In this module the data migration take place without TPA. Here, the clouds directly migrate, the data to the respective end data nodes after having permission from USER to both clouds.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

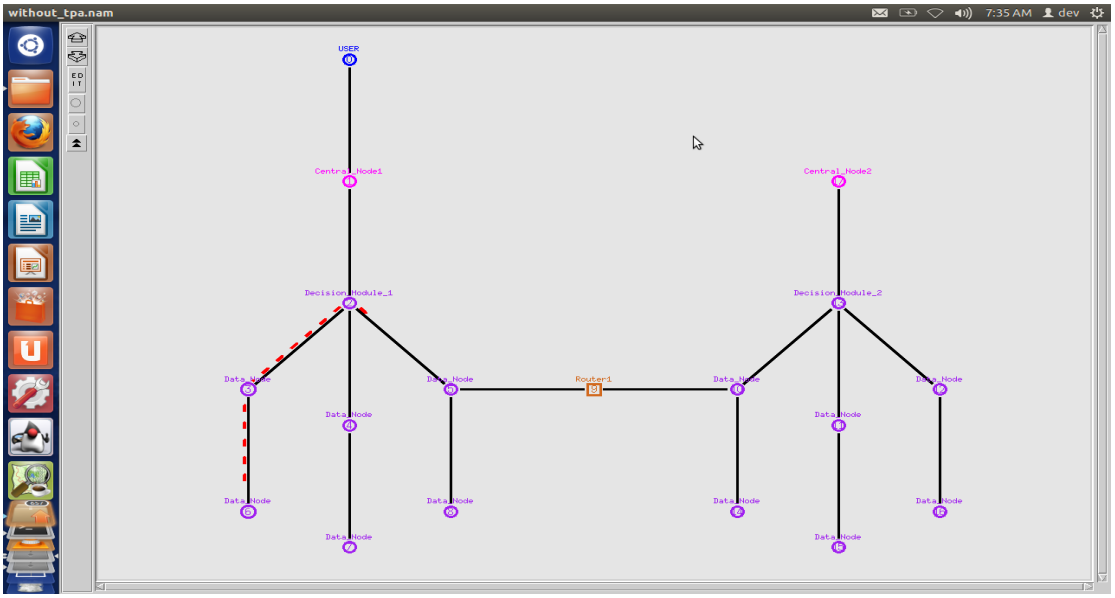

Fig.3: MDM module

Our proposed TPA module is compared with MDM module.MDM module is the migration decision module which is generally performed during data migration at the cloud. This experiment is tested with six different blocks of different sizes.

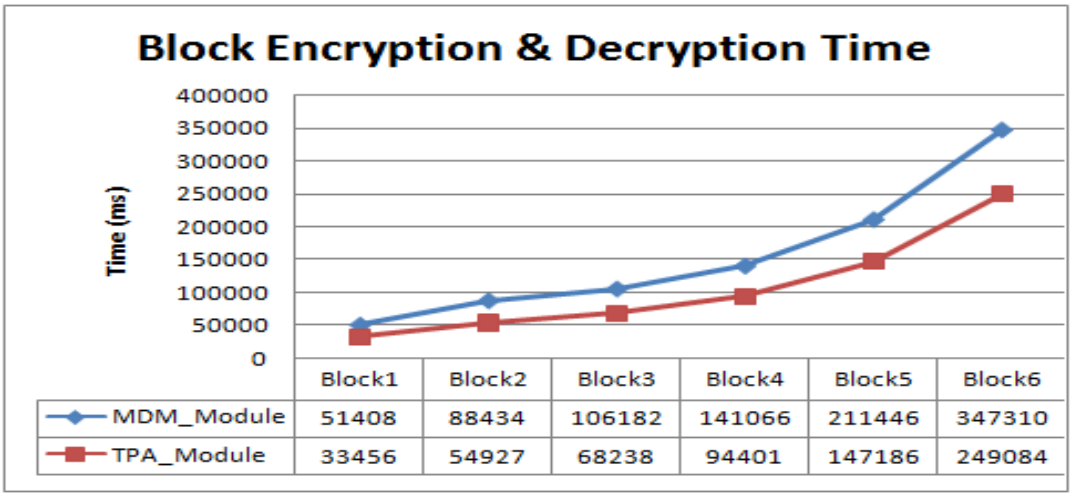

Fig 4: Block encryption and decryption time

Fig.4 shows the Block encryption & decryption time taken during migrating data in TPA module and MDM module. From fig.4 it is clear that our proposed TPA module consumes less time to encrypt and decrypt data compared to the existing MDM module. Accordingly this mechanism is efficient to secure data migration between SSL protocol based cloud storage systems.

V. CONCLUSION

With the importance of cloud computing and its attractive application areas it has still many challenges to overcome. There are number of threats of security from which it can suffer, one of them is faced during data migration. A secured

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

TPA mechanism is proposed which is embedded with the SSL protocol. SSL protocol helps us to share parameter more safely. In this paper, we performed and analysed the block encryption and decryption time phase at two modules TPA and MDM. The simulative results shows that TPA module performs better than MDM module embedded with SSL protocol with better time constraint parameter. As a future work, we will implement a detailed design for authentication framework as private data protecting service based on digital signature and remote attestation.

REFERENCES

[1] Ateniese G., R.Burns, R. Curtmola, J.Herring and L.Kissner et al., "Provable data possession at untrusted stores.", Alexandria, Virginia, USA**,**ACM 978-1-59593-703-2/07/0011,page-598-610,2007.

[2] Wang, C., Q. Wang, K. Ren and W. Lou,"Privacypreserving public auditing for data storage security in cloud computing",IEEE Computer Society, ISSN:0018-9340,Vol.62,Issue 2,page-362-375, 2010.

[3] Venkatesh, M., M.R.Sumalatha and C.Selva Kumar,"Improving public auditability, data possession in data storage security for cloud computing."International Conference on Recent Trends in Information Technology (ICRTIT),IEEE,ISBN:978-1-4673-1599-9, page-463-469,2012.

[4] Sarfraz Nawaz Brohi, Mervat Adib Bamiah, SuriayatiChuprat and Jamalul-lail Ab Manan 2013 "Design and implementation of a privacy preserved off-premises cloud storage". Journal of Computer Science 10 (2): 210-223, 2014, ISSN: 1549-3636, page-210-224, 2014.

[5] Rashmi Rao, Pawan Prakash, "Improving security for data migration in cloud computing using randomized encryption technique "IOSR Journal of Computer Engineering (IOSRJCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727,Volume 11, Issue 6, PP 39-42,2013 .

[6] R.Vinodha, Mr.R.Suresh," Secure Migration of Various Database over A Cross Platform Environment" ,www.ijecs.in International Journal of Engineering and Computer Science, ISSN: 2319-7242 Volume 2 Issue 4 , Page No. 1072 -1076,2013.

[7] Prashant Pant, Sanjiv Thakur,"Data Migration Across the clouds", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[8] Virendra Singh Kushwah, Aradhana Saxena," A Security approach for Data Migration in Cloud", International Journal of Scientific and Research Publications, Volume 3, Issue 5, ISSN 2250-3153,2013.

[9] Wei Hao, I-Ling Yen and Bhavani Thuraisingham,"Dynamic Service and Data Migration in the Clouds", Computer Software and Applications Conference,COMPSAC, 33rd Annual IEEE International Conference, ISSN :0730-3157 , Page:134-139,2009.

[10] K.Meenakshi, Victo Sudha George 2014 " Cloud Server Storage Security Using TPA", International Journal of Advanced Research inComputer Science & Technology (IJARCST), ISSN : 2347 - 9817 (Print), Vol. ,2 Issue Special 1, Jan-March 2014.

[11] Balakrishnan.S, Saranya.G, Shobana.S, Karthikeyan. S 2011 "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud"IJCST,Vol.2, Issue-2ISSN:2229-4333,page-397-400,2011..

[12] D.Srinivas et al. ." Privacy-Preserving Public Auditing In Cloud Storage Security",(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6) ,page-2691-2693, 2011.