www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Volume-5, Issue-3, June-2015

International Journal of Engineering and Management Research

Page Number: 432-435

A Survey on Data Migration Techniques Across the Cloud Storage Systems

Shyamli Dewan[1], Devendra Kumar[2], Sandeep Gonnade[3], Nilmani Verma[4]
[1,2]M. Tech. Scholar, CSE Department, School of Engineering & IT, MATS University, Raipur, INDIA.
[3]Assistnat Professor, CSE Department, School of Engineering & IT, MATS University, Raipur, INDIA.
[4] H.O.D., CSE Department, School of Engineering & IT, MATS University, Raipur, INDIA.

ABSTRACT

In cloud computing, the data could be stored anywhere across the globe, and it limits the client organisations to have less control over the stored data. In cloud computing, it is seen many times that user data is altered, deleted or modified. A data migration technique is adapted by users to have better security services like third party auditor, to ensure that their data is safe on the cloud. So there is need of more secure mechanism to migrate the data over the cloud and hence several mechanisms have been proposed. This paper presents the literature survey related to data migration techniques available across the cloud storage systems.

***Keywords*-----** Cloud Computing, Privacy, Data Migration,TPA

I. INTRODUCTION

Cloud computing depicts the collection of formal entities like software, music, data etc., which are convenient to be use via internet. Generally, the data is stored in banks of servers spread across the globe from the client side. Traditionally, software like a paint brush or media player required a license to be installed on client's machine. This made the client-server model arrived to existence, which provided large storing capabilities allowing users to host applications with data for workgroup, and hence workgroup became more highlighting. The client machine would use client CPU and memory for processing and would demand a browser to get into the server demanding particular services like e-mail, movies, music etc. Cloud providers liberated the client from software license agreement etc, since the services offered are convenient to be use via internet. Cloud company providers now provide Software as a Service (SaaS), which require a browser enabled devices like desktop computers, laptops, and latest devices like Smartphone, tablets etc, to access these services. An individual needs to be registered with the cloud to use the facility of cloud. After successful registration with cloud, an individual can opt for storage service from the cloud provider, and then she or he can upload personal information, code, music, movies, songs, photographs, which are stored anywhere across the planet in the server bank under Cloud Company. Usually the geographic storage location of servers is kept unknown to the user. There are three basic service models of the cloud computing are (Figure 1):

SaaS

Software as a Service (SaaS) allows client user to use software services supplied by cloud provider via web browser over the internet. Cloud service provider is responsible for the management of server, internal cloud network, operating system, application configuration on middleware etc. It is also known as "on-demand software" service. SalesForce is one of cloud company which supplies different software services using SaaS platform .

PaaS

Platform as a Service (PaaS) provides a platform for deployment of user application, but doesn't give control of hardware or infrastructure (storage, network) implicitly.

IaaS

Infrastructure as a Service (IaaS) provides limited accessibility for infrastructure to the client for storage, network, processing etc. The user can deploy and execute applications using these infrastructures. The main advantage of IaaS platform is that it frees the client user on buys or purchasing top end servers' softwares, data-center

space, network infrastructure etc. Usually the clients are charged on per-use basis.

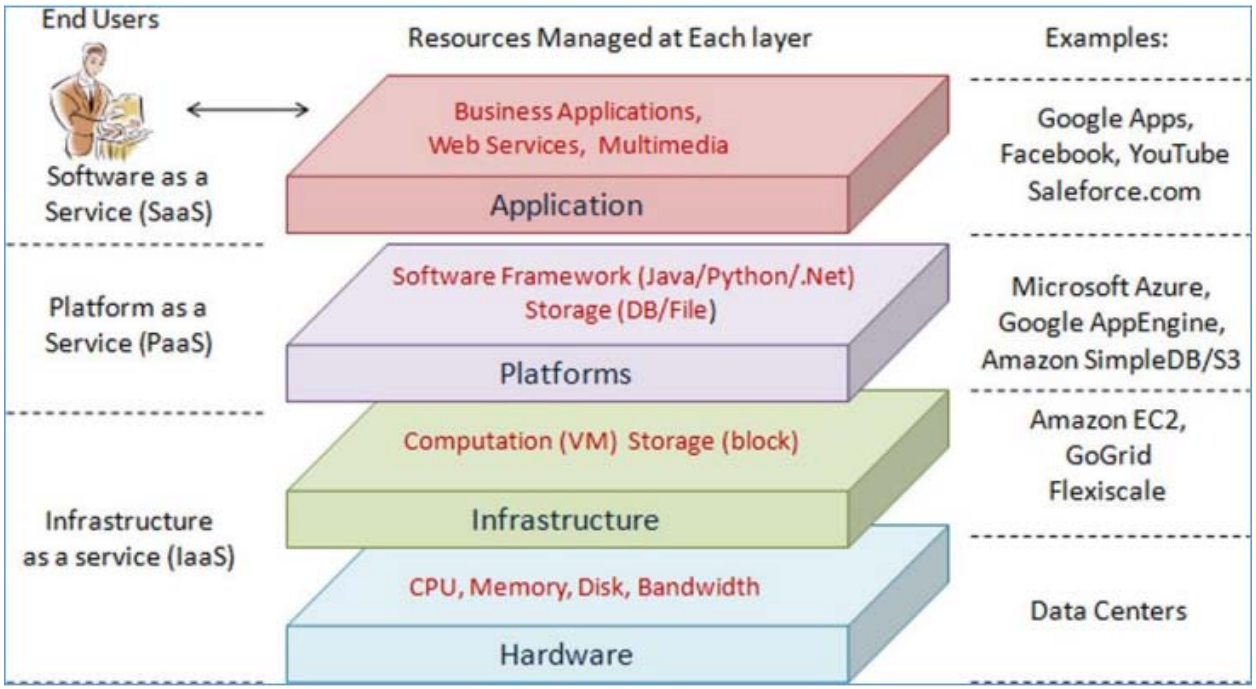

Fig1: A layered model of Cloud Computing [19]

II. DATA MIGRATION

Currently, there are many cloud storage systems like HDFS, Amazon's S3 which provide data migration service to cloud users. But they do not ensure the security mechanism to protect the user data completely and safely. The cloud providers do not take into account the potential threats brought during the process of data migration [1, 2, 3].

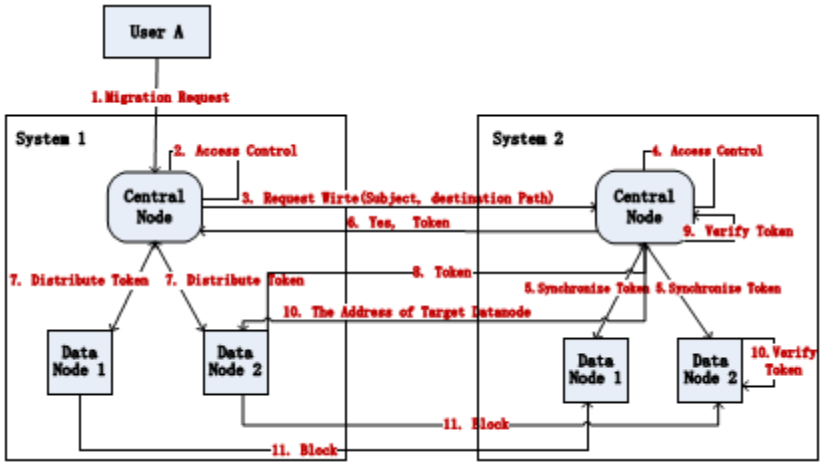

Fig2: Data migration from Cloud storage system1 to Cloud storage system2 [8]

Figure 2 depicts the process of data migration between Cloud Storage System 1 and Cloud Storage System 2. Three kinds of entities are involved in the migration process as shown in Figure 2 [3, 4, 5, 6, 7].

User A: User A sends the migration request to its storage service provider [8].

Central Node: The central node is responsible for accepting user's command to start the migration process and to accept the read request from the data node in the source cloud and return location information; The central node of the target cloud is responsible for processing write requests from Data Nodes[8].

Data Node: Data node is mainly responsible for storing data and processing data request from its Central Node. The program running in the Data Node of the source cloud is started by the Central Node. This program gets location information of inputting files and outputting files. The former is from the source Central Node and the later is from the target Central node. At last, Data nodes migrate the files to the target cloud according the location information [8].

III. LITERATURE SURVEY

Abhishek Mohta et.al. [9] proposed Virtual machines, which uses RSA algorithm for client data/file encryption and decryptions. It also uses SHA-512 algorithm which makes message digest and check the data integrity. The Digital signature is used as an identity measure for client or data owner. It solves the problem of integrity, unauthorized access, privacy and consistency.

K Govinda et.al. [10] proposed digital signature method to protect the privacy and integrity of data. It uses RSA algorithm for encryption and decryption which follows the process of digital signatures for message authentication. But the authors are not able to address the TPA Protocol for exact dynamic auditing.

S. Marium et.al. [11] proposed Extensible authentication protocol (EAP) through three ways hand shake with RSA. They proposed identity based signature for hierarchical architecture. They provide an authentication protocol for cloud computing (APCC). APCC is more lightweight and efficient as compared to SSL authentication protocol. In this, Challenge handshake authentication protocol (CHAP) is used for authentication. The Service provider authenticator (SPA) sends the first request for client identity. To provide security, asymmetric key encryption (RSA) algorithm is used.

Dhiyanesh [12] proposed MAC based and signature based schemes for realizing data audit ability and during auditing phase data owner provides a secret key to cloud server and ask for a MAC key for verification. They are exposed to TPA. Due to this local data content are not preserved as private.

Bal Krishna et.al. [13] proposed efficient Solomon technique for error correction which check data storage correctness. When an unauthorized user access user data, a small application runs which monitors user inputs, it matches the user input, if it is matched then it allow user to access the data otherwise it will block protocol automatically. It contains five algorithms as keygen, SinGen, GenProof, VerifyProof, Protocol Verifier. Protocol Verifier is used by CS. It contains three phases as Setup, Audit and PBlock.

Jachak K.B. et.al.[14] proposed privacy preserving Third party auditing without data encryption. It uses a linear combination of sampled block in the servers response is masked with randomly generated by a pseudo random function (PRF). It involves more computation not dealing with dynamic auditing.

Cong Wang et.al. [15] proposed privacy preserving public auditing which allows TPA along with user to check the integrity of the outsourced data stored on a cloud and Privacy Preserving allows TPA to do auditing without requesting for local copy of the data. Through this scheme, TPA can audit the data and cloud data privacy is maintained. The analysis shows that they are not providing any security for cloud data storage.

Kan Yang et.al. [16] proposed efficient and secure dynamic auditing protocol for data storage in cloud computing. Designed an auditing framework for cloud storage systems and proposed an efficient and privacy-preserving auditing protocol by extending the protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. Resolved reply attack with the help of index table structure and forge attack by modifying the Tag in dynamic data updating.

In Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li [17], the authors proposed a dynamic auditing protocol that can support the dynamic operations of the data on the cloud servers, but this method may leak the data content to the auditor because it requires the server to send the linear combinations of data blocks to the auditor.

In Yan Zhu used et.al. [18] a quantified new audit approach based on probabilistic queries and periodic verification, as well as an optimization method of parameters of cloud audit services. This approach greatly reduces the workload on the storage servers, while still achieves the detection of servers' misbehavior with a high probability.

IV. CONCLUSION & FUTURE WORK

From literature survey it could be seen that how delegation of responsibility trusted third party is required to provide security services to secure client user data. It allows the client for using any browser enabled device to access the cloud services and reliefs the client from

maintaining any kind of key information. It allows the client to verify the integrity of the data stored on download or retrieval of its own stored data in cloud during the process of migration.

Although, there are severe security solutions are proposed for migrating data from one cloud to another. It is decidable by the user that how he/she decide to move/migrate their applications and services to Cloud. If the client user decides to migrate their businesses data to the Cloud, they need to consider a number of risks and threats that may arise. The client user may recommend some best practices and solutions to protect their applications, services and data from those risks which may be helpful when the users want to migrate their applications in the Cloud.

The future work can be carried out to enhance the security mechanism to secure the keys in cloud computing. Further the overhead of network traffic can be reduced, may be another area of research.

REFERENCES

[1] Amazon.com, "Amazon Web Services (AWS), " Online at http://aws.amazon.com, 2008.

[2] W. Cong, Q. Wang, K. Ren, W. Lou, "Ensuring data storage security in cloud computing,"In: Proc. of IWQoS 2009, 2009, pp. 1-9.

[3] Owen O'Malley, Kan Zhang, Sanjay Radia, Ram Marti, and Christopher Harrel "Hadoop Security Design". Technical Report, 2009-10.

[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple- Replica Provable Data Possession, " Proc. of ICDCS '08, pp. 411-420, 2008.

[5] J. Dean and S. Ghemawat. Mapreduce: Simplied data processing on large clusters. In Proc. OSDI, 2004.

[6] Konstantin Shvachko, Hairong Kuang, Sanjay Radia, Robert Chansler. The Hadoop Distributed File System. In Proceedings of the 26th IEEE Symposium on Mass Storage Systems and Technologies, pp: 1~10, 3-7 May 2010, Incline Village, NV.

[7] Qingni Shen, Lizhe Zhang, Xin Yang, Yahui Yang, Zhonghai Wu, Ying Zhang, "SecDM: Securing Data Migration Between Cloud Storage Systems", Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing,pp-636-641,2011.

[8] Abhishek Mohta, Lalit Kumar Awasti, "Cloud Data Security while using Third Party Auditor", International Journal of Scientific & Engineering Research, Volume 3, Issue 6, ISSN 2229-8 June 2012.

[9] K Govinda, V. Gurunathprasad and H. sathishkumar, "Third Party Auditing for Secure Data Storage in Cloud Through Digital Signature Using RSA", International Journal of Advanced science and Technical Research, vol. 4, no. 2, ISSN: 2249-9954,4 August 2012.

[10] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, "Implementation of EAP with RSA for Enhancing The Security of Cloud Computig", International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012.

[11] B. Dhiyanesh "A Novel Third Party Auditability and Dynamic Based Security in Cloud Computing" , International Journal of Advanced Research in Technology, vol. 1,no. 1, pp. 29-33, ISSN: 6602 3127, 2011.

[12] Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan. S,"Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976-8491(Online), June 2012.

[13] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J. "Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing", Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012.

[14] C wang, Sherman S. M. Chow, Q. Wang, K Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Trasaction on Computers I, vol. 62, no. 2, pp.362-375 , February 2013.

[15] Kan Yang and Xiaohua Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp.1717-1726, September 2013.

[16] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.

[17] Yan Zhua,b, Hongxin Huc, Gail-Joon Ahnc, Stephen S. Yauc. "Efficient audit service outsourcing for data integrity in clouds" in "The Journal of Systems and Software 85 (2012) 1083– 1095",2012.

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