IJCTA, 8(2), 2015, pp. 381-389

Privacy Proof of Data Transportability from one Cloud to another Cloud Service Provider

Rama Krishnan[*] and V. Mathivanan[**]

Abstract: In the terms of data portability in cloud environment is highly demanded task. Nowadays, organization and people are smart to find best cloud service with low cost, high efficiency and tight security. They are always enquiring with numerous of cloud service provider against quality of services. In existing some of the method provided approach for data migration form one cloud to another cloud server. However, existing approach are still susceptible due to weak security. To overcome the issue, this paper presents Efficient and Secure Cloud Data Migration (ESCDM) Algorithm to migrate owner data from one cloud to another cloud. Proposed approach migrate the data from one cloud to another after the confirmation from data owner side. It provides authentication key to data owner to edit and update his/her data. Proposed method also assists to data owner to reduce duplication and misleading of data by updating the key. Once, cloud server receives confirmation from data owner then it encrypts the data and forward to requested location. Experimental results shows that proposed mechanism have perform well on data transportation time, data retrieval time and messages cost against existing approaches.

Keywords: Data transportability, data owner, efficient and secure cloud data migration (ESCDM) algorithm, data transportation time, retrieval time, message cost.

1. INTRODUCTION

In recent existence, the upcoming cloud computing prototype is rapidly gaining momentum as an alternative to usual information technology. Cloud compute provide a scalability atmosphere for on the rise amounts of data and processes that work on various applications and services by means of on-demand self-services. One essential aspect of this model changing is that data are being centralized and out sourced into clouds. These kinds of outsourced storage services in cloud environment which become a new profit growth point by providing a comparably less-price, scalable, locality-independent stage for managing owner's data.

Proof of Retrievability (POR) and Proof of Data Possession (PDP) techniques confirm data integrity for cloud storage. Proof of Ownership (POW) enhances storage efficiency and removing unnecessarily duplicated content storage server [17]. However, trivial combination of the two techniques, in order to achieve both data integrity and storage efficiency is non-trivial of data duplication (i.e., authentication tags). In the terms of data portability in cloud environment is highly demanded task because nowadays, organization or client are too smart to find best cloud service with low cost, high efficiency and tight security of data. They always verify with numerous of cloud service provider against quality of services [6]. To reduce the cost, and improve efficiency of application, they plan to change the cloud server. In this scenario, owner has to receive all his/her data in physical storage from Cloud Service provider. Hence, data owner can upload his/her data with new CSP. In existing some of the method provided to direct data migration form one CSP to another CSP. However, existing methods are still susceptible to security threats both from outside and inside the cloud. They did not consider privacy issues with efficiency during data

[*] Research Scholar, Dept. of Computer Science & Engineering, AMIET University ECR, Kanathur, Chennai, India, *E-mail: ramakrishnanr@gmail.com*

[**] Research Supervisor, Research Scholar, Dept. of Computer Science & Engineering, AMIET University ECR, Kanathur, Chennai, India, *E-mail: vmathivanan@yahoo.com*

transportation. Even though, they had not provide any mechanism where data owner authenticate privacy or update security of data.

To overcome the issues, paper present Efficient and Secure Cloud Data Migration (ESCDM) to transport owner data from one CSP to another CSP. This method transports the data from one cloud to another after the confirmation from owner side. It provides authentication key to data owner to manage his/her data. In this process, data owner have full authority to edit and update his/her data in cloud environment. Hence, it encrypts the data and forward to requested location. Once, data store in new CSP. Hence, proposed method send notification and data encrypted key. Proposed algorithm protects owner's data from malicious attack. Paper contributions of work follow as:

1. Proposed method transport the data from once CSP to another CSP with high efficiency and low privacy complexities after getting confirmation mail.
2. Proposed methods encrypt owner data and update the key data owner. Hence, data owner can save his data from duplication by updating key of data.
3. Proposed approach avoids external or internal attack of owner data.
4. It reduces traffic and unnecessary utilization of physical storage.
5. Experimental results displays that the proposed approach performs well on data transportation with tight security for entire process.

The rest of paper follows as: In section 2, we mentioned literature review which is close to proposed mechanism. In section 3 introduces the p system model with proposed techniques elaboration. In Section 4, explain about experimental result and discussion. In section 5, concluded the overall work with future enhancement.

2. LITERATURE REVIEW

In this paper [1] author developed usage of Multi-Agent System (MAS) techniques that can be beneficial in cloud computing platform to facilitate security of cloud data storage (CDS) with it. MAS are often rotated and agents have proactive and reactive features which can be utilized for cloud data storage security (CDSS). The architecture of the system is build up from a set of agent's groups. This paper of literature review described on the theoretical concept and approach of a security framework as well as a MAS architecture that could be implemented in cloud platform in order to facilitate safety of CDS, on how the MAS skill could be utilized in a cloud platform for serving the security that is developed by using a collaborative environment of Java Agent Development (JADE). In this paper [2], author presented an original data recovery service framework on cloud infrastructure, a Parity Cloud Service (PCS) that provide a privacy-protected personal data revitalization service. Newly developed framework does not require any user data to be uploaded to the server for data recuperation. Also the resource of server-side is obligatory for providing the service is within a reasonable bound. In paper [3], author developed a entire service named SSTreasury+ which includes encryption application and cloud storage space service. The user's data quicker than uploading to cloud environment could be encrypted first to prevent the data to be stolen during transmission or in the cloud storage space. In this paper [4], author developed a framework that would provide integrity of data of multiple users through Third Party Auditor (TPA) and developed various algorithms to implement this framework. In the developed framework concept of multi cloud has been used to provide best cost optimization for various needs of user. This framework is also classified into three platforms namely: platinum for sensitive information storage, gold for minimum security and silver for least level of security on the data. Finally author has implemented different algorithms for the various platforms in the developed framework. In this paper [5], author designed an auditing framework for cloud storage systems and developed an efficient and privacy-preserving auditing protocol. Then, author extends our auditing protocol to support the data progressive operations, which is capable and provably protected in the random oracle model. Author further expand their auditing protocol to assist batch auditing for both multiple owners and various clouds, without using any faithful organizer. In this paper [6], author developed a smart remote data backup plan using Seed Block Algorithm (SBA) with Advance Encryption Standard (AES) algorithm. In case if the some data gets removed due to any reason, AES helps to recover that file from a backup file which is stored at a remote location. The time related issues are also being solved by method such that it will take minimum time for the recovery process. In this review paper [7], author explored few recent techniques that are the powerful solutions in the form of “Online Data Backup and Disaster recuperation methods”. The purpose of this review paper is to summarize the powerful data backup recovery techniques that are used in cloud computing domain

The purpose of recuperation technique is to help user to collect information from any backup server when server lost his data and unable to provide information to the user. In this paper [8] author introduced a model for the integrity checking over the cloud computing with the support of the TPA utilizing digital signature technique. The model result was displayed efficiently with a number of situations that performed by unconstitutional assailant. The inspection done over two parts the CSP and TPA, without philanthropic any protected information that negated the integrity definition and without uploading any secure data to the cloud. In this paper [9], author developed a smart remote data backup algorithm, Seed Block Algorithm (SBA). The objective of new algorithm was twofold; first it help the users to collect information from any remote location in the absence of network connectivity and second to recover the files in case of the file deletion or if the cloud gets destroyed due to any basis. The time associated problems is also being make out by new SBA such that it will take minimum time for the recovery process. In this paper [10], author worked on crams problem of make sure the reliability of data storage in Cloud Computing. In particular, author considers the task of allowing a third party auditor (TPA), on behalf of the cloud client, to clarify the integrity of the metadata stored in the cloud server. The introduction of TPA reduces the involvement of the client through the auditing of whether his data stored in the cloud or not which can be significant in attain financial system of scale for Cloud Computing. In this paper [11], author focused on privacy of cloud. Everyone is applying on security algorithms like encryption decryption and all, but author were many approaches which is far better than the security algorithms. Have to implement security part. The method is like this data is divided into small segments and store in all different cloud related with each other and that cloud will store data into different servers and those server will save data into different database and those database will store data into different disk.

In this paper [12], author developed a capable and safe protocol to address this concern. Author’s plan is based on Elliptic camber Cryptography and Sobol progression (random sampling). Presented method allows third party inspector to sporadically verify the data veracity stored at CSP without get back original data. It engenders probabilistic testimony of veracity by challenging unsystematic sets of blocks from the server, which hugely reduces the communication and I/O costs. In this paper [13], author designed a cipher text-policy attribute-based encryption (ABE) scheme and a proxy re-encryption scheme. Based on them, author further developed a secure, efficient and fine-grained data Access Control mechanism for Peer-to-Peer computing storage Cloud named ACPC. Enforce authentication policies based on user attributes, and integrated P2P reputation system in ACPC. ACPC allow information owners to farm out most of the laborious user revocation tasks to cloud servers and reputable scheme peers. In this paper [14], author developed simple mechanisms that enable cross-user de-duplication while greatly reducing the risk of data leakage. It demonstrates how de-duplication can be used as a side channel which reveals information about the contents of files of other users. In a different scenario, de-duplication can be used as a covert channel by which malicious software can communicate with it’s manage center, in spite of any firewall setting at the attack mechanism. In this paper [15], author developed an encryption algorithm to address the safety and privacy issue in cloud storage in order to defend the data stored in the cloud. In this paper [16], author implemented a comprehensive security framework based on Multi-Agent System (MAS) architecture for CDS to facilitate privacy, rightness pledge, ease of use and veracity of users' data in the cloud is developed. In order to verify our new safety framework based on MAS structural design, pilot study is behavior using a survey. To replicate the agents, oracle database correspondence and triggers are used to implement agent function and prophesy jobs are exploiting to create agents.

3. SYSTEM MODEL

In this phase, represents about novel system model, merit with implemented function. Here, model implemented procedure is classified in the phase namely: data owner, cloud server provider, data transportability and Efficient and secure cloud data migration (ESCDM) algorithm System model elaborates working function in figure 1. In phase, proposed approach represent data migration model in multiple cloud environment. This method avoids external malicious attack during data migration from one cloud to another cloud server.

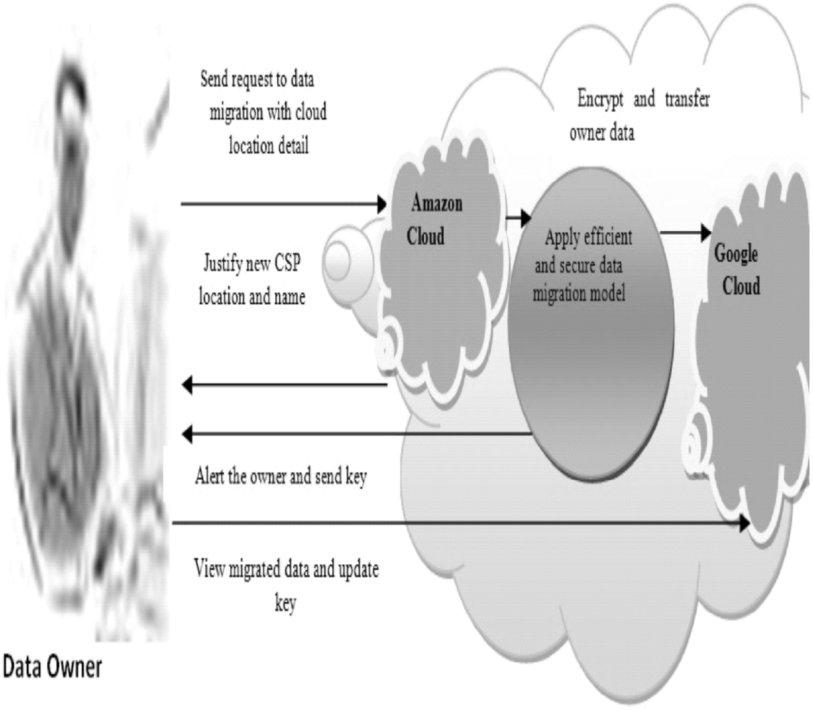
Send request to data migration with cloud location detail
Encrypt and transfer owner data
Amazon Cloud
Apply efficient and secure data migration model
Google Cloud
Justify new CSP location and name
Alert the owner and send key
View migrated data and update key
Data Owner

Figure 1: System workflow design

3.1. Data Owner

In this module, the Data owner wishes to upload or publish his/her data to the cloud server so that t users can access and data. Data owner contains set of original data and a key which can be used for data transformation in cloud. Data owner has full access to change his/her CSP anytime.

3.2. Cloud Service Provider

In this module, a CSP who manages cloud application services based data owner request. CSP provides services to databases based on Software Legal Agreement (SLA). CSP assist paid services to owner's application customer based on his/her demand. If owner is not satisfied CSP and he wants to change CSP then CSP would have to transfer the owner application on requested location. But, its only happens when data owner will send confirmation to respected CSP.

3.3. Data Transportability

Data transportation is a process to migrate the large volume of owner's data from once cloud service provider to another cloud service provider. Since large volume of applications is responsible fulfill an industry's business requirement to achieve the growth. Now, they are variety of DaaS (Database as a service) are available to keeping in view of data migration process. However, migration is a not simple task in cloud due lack of data integrity, confidentiality, security, portability, and data accuracy issues.

3.4. Efficient and Secure Cloud Data Migration Algorithm

Data transportability is one of the biggest advantages in cloud environment. In this ways, user takes his/her PC backup and store in cloud. However, this feature is not much effective without proper privacy of data. To fulfill the current needs, papers presented Efficient and secure cloud data migration (ESCDM) algorithms. It provides tight security of owner during migration process. In this phase, proposed approach take care full securities from data transportation to data retrieval. Once old server start to transfer the data then proposed approach will encrypts the data and hence allow to process for migration. Once, data reach the destination place, its alert to owner and send encrypted key. Now owner access the migrated data. It provides feature to owner to update data with new key. When data update will new key then old server can access and view the owner if he also has duplicate of application.

Proposed techniques verify the size of container. It clarify maximum and minimum container of migrated data. Hence, it allow for transportation process. Next its moves to verification for requested server whether it is public cloud or public or private cloud. Hence, it proceeds to justify owner profile and background. Finally encryption process encrypts and transports the data. Here, encryption and decryption is necessary to reduce the transportation time and enhancement of data privacy. Proposed algorithm sends notification to owner with authentication key. Proposed algorithm pseudo code is described below in details in figure 2.

```
Variable Select Minimum
Variable Select Maximum
Method Containersize { Containersize.MC=Random((Selectmin,Selectmax)
}
Method Migrateddata { Sum(Containersize.Unique+Date.Unixtime+Serverinstance.Hexvalue+Owner.Hexvalue)
}
Method Decrypt
 {
Datadecryption Method
}
Containersize.Unique = Callmethod Containersize+0.075%
Insert Containersize.Unique
Locate Date.Unixtime
Select Serverinstance
Convert Serverinstance.Hexvalue
If Instance = Publiccloud
{
Select Ownername Convert Owner.Hexvalue
 }
Else Owner.Hexvalue=0
Callmethod Migrateddata
DataContainer.Unique=Append (Container. Containersize+Migrateddata)
Number (Id.Unique) = New Id DataContainer.Unique DataContainer.Unique =DataContainer.Unique+Id.Unique
Insert DataContainer.Unique Into Migratedata.Security
Encrypt DataContainer.Unique
If Report.Initiated
{
Call Method Decrypt (DataContainer.Unique)
}
```

Figure 2: Pseudo code for Efficient and secure cloud data migration algorithm

4. RESULT AND DISCUSSION

4.1. Experimental Setup

In order to compares proposed mechanism with existing algorithm. This paper utilized jelastic open source cloud server. The experiment is conducted on a laptop with Intel Dual Core processor with 1GB memory, and Window 7 Ultimate system. Here, this method implement in JAVA using NetBeans 8.0 with JProfiler and JPA plug-in and MYSQL 5.5 database.

4.1.1. Data

For proposed approach evaluation, the experimental system utilized 3 kinds of data 100KB, 1MB and 100 MB database. For migrating the owner data from one cloud server to another cloud used JAVA based effective and secure migration model.

4.2. Result

In this phase, proposed Efficient and secure cloud data migration algorithm represent mathematical model to evaluate the performance of data transfer time, and data retrieval time with tight security.

4.2.1 Data Transportation Time

In this section, proposed approach elaborate mathematical model for data transportation time in equation (1).In this step, method calculates as transportation time with encryption of owner data. Data transpiration time (DTT) is calculated as:

$$DTT = T_{enc} + \left(T_{end} - T_{start}\right) \tag{1}$$

Where T_{enc}= total time taken by method to encrypt the data. Where T_{end} is data transportation completion time and T_{start} is initial time of data transportation process.

4.2.2. Data Retrieval Time

In this section, proposed method describes mathematical model for data retrieval time in equation (2). In this step, method calculates as retrieval time with decryption of owner data. Data retrieval time (DRT) is calculated as:

$$DRT = \frac{\left(T_{finished} - T_{proces\sin g}\right)}{ONCSP_{bandwidth}} + T_{decrpt} \tag{2}$$

Where $T_{finished}$= total time taken by method to retrieved the data. Where $T_{processing}$ is data processing to access & view the data and $T_{decrypt}$ is decryption time to retrieve the data in original view. Here $ONCSP_{bandwidth}$ is new cloud service provider bandwidth which is recently selected owner to get reliable service

4.2.3. Message Cost

In this section, proposed approach explain mathematical model in equation (3) to message cost (%). The message cost (MC) is calculated as respected of message transfer rate with message content sizes.

$$MC = \frac{MR_{transfer}}{MCon_{size}} \times 100$$

Where $MR_{transfer}$ is message transfer rate and $MCon_{size}$ is total size of message content

Table 1 represents Message cost (MC), Data Transportation Time (DTT) in sec and Data Retrieval Time (DRT) in milliseconds for 100KB, 1MB and 100 MB dataset. We measure the communication cost (in %), uploading time (in sec), and query retrieval time (in msec) and we display their average values for respective parameter with respective dataset

Table 1
Message Cost (MC), Data Transportation Time (DTT) and Data Retrieval Time (DRT) for 100kb, 1mb And 100 Mb Dataset

Learning Algorithms	*100KB*			*1MB*			*100MB*		
	MC	*DTT*	*DRT*	*MC*	*DTT*	*DRT*	*MC*	*DTT*	*DRT*
MHT	97	6.45	808.1	95	8.45	995	96	9.20	1200
SBA	96	3	1300	95	5	900	93	7	1500
PCAD	95	1.81	900	93	3.81	1200	88	5.25	1445
ESCDM	100	1	500	99	2.25	700	98	3.95	900

According to proposed Efficient and secure cloud data migration algorithm performance result in figure 3, 4 and 5 for 100KB, 1MB and 100MB dataset. ESCDM is the best approach. In terms of message cost, paper nearest competitor is MHT [10]. In the terms of data transportation time, paper nearest competitor is PCAD [17]. In the terms of data retrieval time, paper nearest competitor is MHT [10]. However, proposed method reduce the DTT is 1.22 sec and reduce DRT is 301mili second for overall dataset. It also enhances message cost performance 3% compare than existing methods for all dataset. Finally, paper claim that ESCDM is the best approach for all dataset.

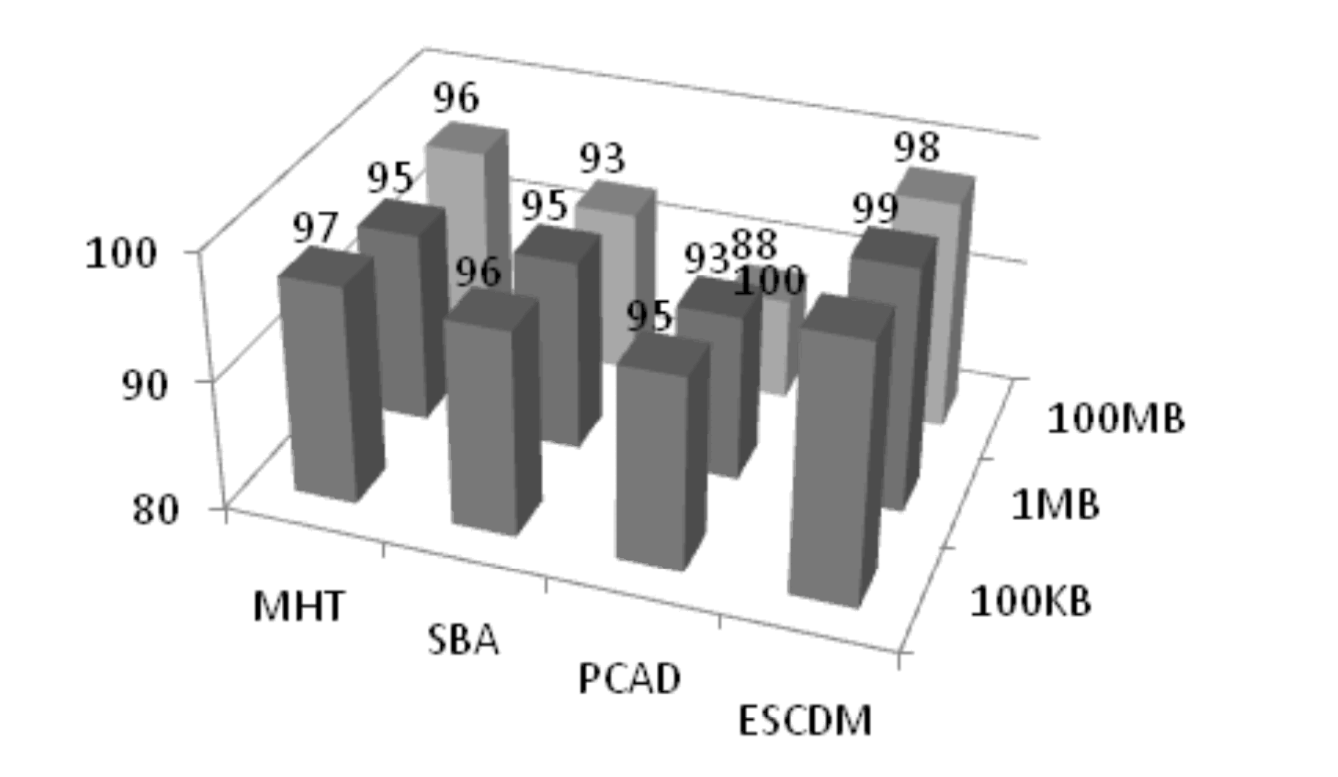

Figure 3: Message cost for 100KB, 1MB and 100MB dataset

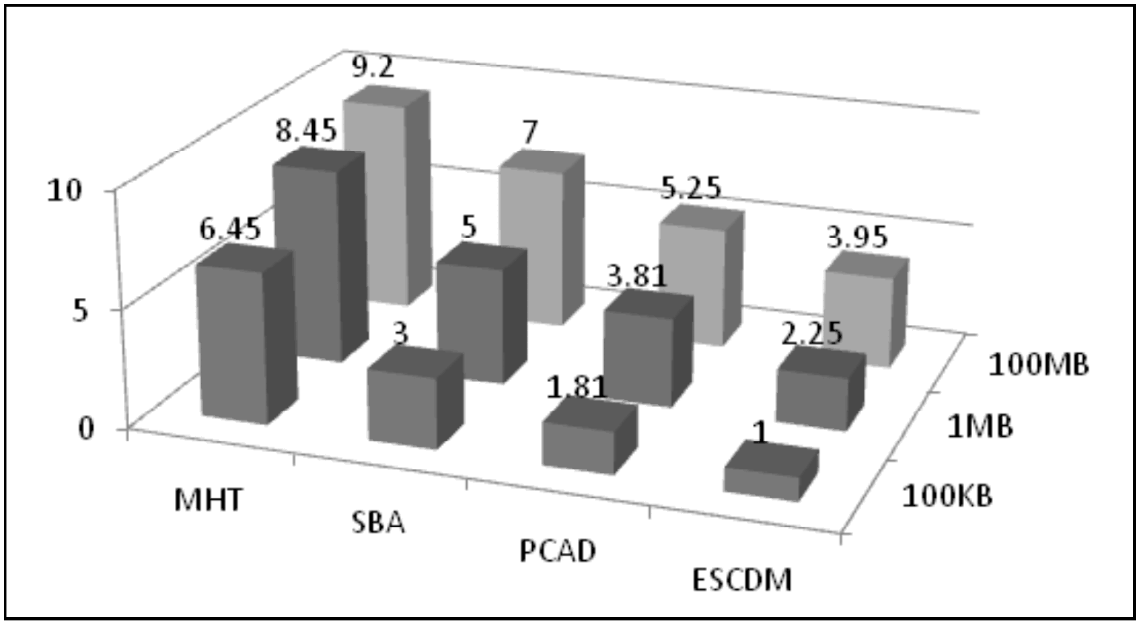

Figure 4: Data transportation time (sec) for 100KB, 1MB and 100MB dataset

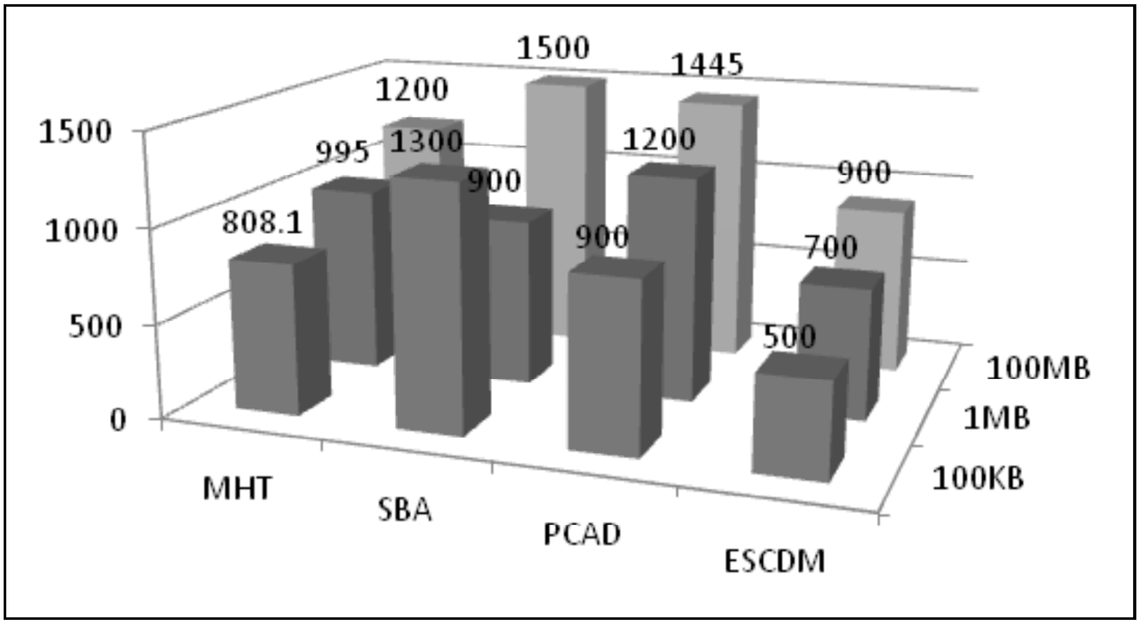

Figure 5: Retrieval time (msec) for 100KB, 1MB and 100MB dataset

5. CONCLUSION

To alleviate the issues, this paper presents efficient and secure data migration algorithm to migrate owner data from one cloud to another cloud with improved privacy. This methodology starts its process of migration only after getting confirmation from the data owner. Once data owner confirms then proposed approach encrypts the data and transferred on requested CSP location. Once, data transportation process completes then it will send acknowledgement with authentication key to data owner. Now, Data owner can view file details and update the key for migrated data to improve security. Once, data owner update the key then old CSP is unable to view or access the data. Hence, it’s clear that proposed method also assists the data owner to avoid duplication or misleading of data by updating the key. In the terms of message cost, data transportation time and data retrieval time, proposed approach performed well such that data transportation and retrieval delay are reduced to certain level along with enhanced security level. According to experimental results, shows that proposed ESCDM method reduce the DTT is 1.22 sec and reduce DRT is 301mili second for overall dataset. It also enhances message cost performance by 3% compared to other existing methods for all dataset.

This paper also pays way as a future enhancement in the domain of data migration in multi- cloud environments along with multiple platforms and stronger security.

REFFERENCES

[1] A.D. Talib, A. M., Atan, R., Abdullah, R., & Murad, M. A. A., "Security framework of cloud data storage based on multi agent system architecture": Semantic literature review. *Computer and Information Science*, Volume 3, issue 4, pp.175-186, 2010.

[2] Song, C. W., Park, S., Kim, D. W., & Kang, S., "Parity cloud service: a privacy-protected personal data recovery service." In *Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 10th International Conference*, pp.812-817, 2011.

[3] Huang, K. Y., Luo, G. H., & Yuan, S. M., "SSTreasury+: A secure and elastic cloud data encryption system." In *Genetic and Evolutionary Computing (ICGEC), 2012 Sixth International Conference on* IEEE, pp.518-521, 2012.

[4] Thakur, A. S., & Gupta, P. K., "Framework to Improve Data Integrity in Multi Cloud Environment." *International Journal of Computer Applications* (0975 – 8887) Volume 87 – issue: 10, pp.28-32, 2014.

[5] Yang, K., & Jia, X., "An efficient and secure dynamic auditing protocol for data storage in cloud computing." *IEEE Transactions on Parallel and Distributed Systems*, volume *24*, issue 9, pp.1717-1726, 2013.

[6] Tanay Kulkarni, Krupali Dhaygude, Sumit Memane, Onkar Nene., "Intelligent Cloud Back-Up System" *International Journal of Emerging Engineering Research and Technology* Volume 2, Issue 7, October 2014, pp.82-89,2014.

[7] Sharma, K., & Singh, K. R., "Online data back-up and disaster recovery techniques in cloud computing": A review. *International Journal of Engineering and Innovative Technology (IJEIT)*, Volume: 2, Issue: 5, pp.249-254, 2012.

[8] Attas, D., & Batrafi, O., "Efficient integrity checking technique for securing client data in cloud computing." *International Journal of Electrical & Computer Sciences IJECS-IJENS*Volume: 11 issue: 05, pp.43-48, 2011.

[9] Sharma, K., & Singh, K. R., "Seed Block Algorithm: A Remote Smart Data Back-up Technique for Cloud Computing." In *Communication Systems and Network Technologies (CSNT), 2013 International Conference on* IEEE, pp.376-380, 2013.

[10] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J., Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE Transactions on Parallel and Distributed Systems*, volume22, *issue* 5, pp.847-859, 2011.

[11] Tewari, M., & Yadav.A. K. "Distributed Security on Cloud: Mobile Cloud Operating System."*International Journal of Computer Trends and Technology (IJCTT*) – volume 23, issue 4, pp.180-183, 2015.

[12] Syam Kumar, P., & Subramanian, R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", *International Journal of Computer Science*, volume 8 issue 6, pp.261-274, 2011.

[13] He, H., Li, R., Dong, X., & Zhang, Z., "Secure, Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud." *Cloud Computing, IEEE Transactions on*, volume 2 issue4, pp.471-484, 2014.

[14] Harnik, D., Pinkas, B., & Shulman-Peleg, A., "Side channels in cloud services: Deduplication in cloud storage." *Security & Privacy, IEEE*, volume 8 issue 6, pp.40-47, 2010.

[15] Arockiam, D. L., & Monikandan, S., "Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm. *International Journal of Advanced Research in Computer and Communication Engineering* volume 2, Issue 8, pp.3064-3070.2013.

[16] Talib, A. M., Atan, R., Abdullah, R., & Murad, M. A. A. "Towards a comprehensive security framework of cloud data storage based on multi agent system architecture." *Journal of Information Security*, volume 3, pp.295-306, 2012.

[17] Yuan, J., & Yu, S.,"Secure and constant cost public cloud storage auditing with deduplication". *IEEE Conference on* Communications *and Network Security (CNS)*, pp. 145-153, *2013.*