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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Cloud To Cloud Data Transfer Using Secure Erasure Method

Subramanya HP[1], Dhananjaya V[2]

Student, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bengaluru, India[1]

Professor, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bengaluru, India[2]

ABSTRACT—With the multiplication of distributed storage, outsourced information exchange turns into a basic prerequisite for clients to relocate their outsourced information starting with one cloud then onto the next. Be that as it may, information confidentiality and respectability are enormous worries for clients when their information are moving between two semi-legit mists. In this paper, we propose a SecureOutsourced DataTransfer(SODT)conspire to accomplish secure information movement in distributed storage. SODT allowsuserstomigratetheremotedatafromonecloudtoanother without recovering the information from the previous cloud, to such an extent that the information confidentiality and honesty can be accomplished amid this procedure. What's more, the cloud can perform secure information eradication after the information are relocated by using the intermediary method. At long last, we talk about the security properties including confidentiality and honesty of SODT,and show its efficiency as far as the computational and correspondence overhead. In this paper we are introducing Reed - solomon erasure code which is the intermediatory method to erase the data which is present in the cloud and which is no more in use . We also introduce a proxy who takes care of transferring the data owners data from one cloud to another.

KEYWORDS:Outsourced information, clouds ,Integrity, Proxy, Erasure code.

I. INTRODUCTION

Cloud storage enables clients to remotely store their information on cloud servers and offers the on-request great applications and administrations from a common pool of configurable assets, without the weight of nearby information stockpiling and upkeep. An expanding number of people and companies outsource their information to cloud servers for sparing the cost of obtaining and keeping up capacity gadgets, and getting a charge out of the flexible information access at whenever and from anyplace. 82% of associations grasping distributed storage administrations benefit for lessening expense of IT assets [2]. The quantity of occupants in distributed storage is anticipated to achieve 2 billion by 2018 [3]. Because of the promising business sector prospect, a substantial number of distributed storage administrations have developed, e.g., SkyDrive, Dropbox, Zip Cloud and OneDrive, giving different levels of administrations on get to rate, security, dependability and costs [4]. This focused marvel not just gives clients various alternatives when they want to outsource information, yet additionally conveys chances to move the distributed storage administrations on the off chance that they don't satisfytheircurrentstorageservices.Inaddition,clouddataare habitually exchanged over numerous server farms to ensure the different replication stockpiling and sharing. As per Cisco report [3], the traffic among various mists is anticipated to achieve 9% of aggregate cloud traffic by 2018. One direct answer for accomplish the information exchange for clients is to recover their outsourced information from one cloud and transfer them to thenew one. Shockingly, the clients don't have enough stockpiling assets to incidentally store their recovered information. In this manner, outsourced information exchange turns into a central prerequisite for clients to relocate their information starting with one cloud then onto the next. Be that as it may, it is of significant difficulty to accomplish secure information exchange between two mists, as both distributed storage suppliers may carry on unfaithfully finished the information [5], [6]. As a matter of first importance, the respectability of the outsourced information might be attacked by the distributed storage suppliers [7], [8]. For instance, they may dispose of the information that are once in a while or never went by to lease the space to different clients for financial reasons.

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Moreover, an apathetic cloud may move just a bit of client's required information, since information exchange expends numerous assets and transmission capacity. Besides, it is difficult to keep the information introduction to the distributed storage suppliers [9]. Once the information are transferred to the cloud, the clients lose the physical control over their information. Every one of the information are presented to the distributed storage suppliers and the suppliers can discretionarily get to clients' information. Thirdly, the cloud can keep the duplicates of exchanged information to find potential esteem, prompting the information divulgence mishaps. What's more, the foundation of distributed storage are gone up against with the wide scope of dangers from outside assailants towards information trustworthiness and confidentiality [10]. For example, aggressors may vindictively get to the clients' outsourced information by methods for framework vulnerabilities and programming bugs,or listen in on the correspondence channels to catch the clients' information, when they are exchanging between two mists. In synopsis, the accomplishment of cloud engineering is blocked, if there is no security ensure on the outsourced information amid information stockpiling and exchange forms.

II. RELATED WORK

In secure outsourcing [1] scheme the data in one cloud must be re-encrypted by another cloud by using Proxy re-encryption technique which is not so secure that the decryption key might be traced and the content in the cloud might be recovered. To accomplish the information integrity in cloud storage, a few provable information ownership plans [6], [11] have been proposed, whereusersareallowedtoverifytheintegrityoftheclouddata without recovering the information from the cloud. To acknowledge secure information erasure, Reardon et al. [12] presented a general information erasure approach by using encryption and key wrapping systems and defined a key divulgence chart to display the key age wrapping. Feng et al. [13] proposed a safe information eradication conspire with open verifiability utilizing a TrustedPlatformModule.Unfortunately,theschemesonlyguaranteethatthedataaredeletedirrecoverablyfromaphysicalmedium. To keep the information exposure amid relocation, Cloudsfer [14] uses information encryption procedure to construct a mystery channel between two clouds. In spite of the fact that Cloudsfer gives information security amid the information exchange, it can't guarantee the information integrity and rightness for the information in clouds. To address these issues, Yu et al. [15] proposed a provable information ownership conspire supporting secure information exchange for cloud storage. They use the secretly verifiable provable information ownership plot [16] to enable clients to check the integrity of their information in clouds and plan a randomization system to keep the information divulgence and accomplish secure information eradication. In Yu et al.' plot, the paired length of the qualities, which are utilized to randomize the exchanged information, is equivalent to the span of the information.

III. METHODOLOGY

A. SYSTEM MODEL

The System model of outsourced information exchange includes two elements: clients and clouds. The clients have immense volume of information to store, however restricted information storage assets and registeringcapability they want to lease the virtual storage spaces offered by cloud storage suppliers, as opposed to buy physical storage offices. The clouds have a lot of storage spaces and processing assets,and offer remote information storage administrations to clients in a compensation as-you-utilize way. As showed in Fig.1, when a client needs to outsource the information, he/she picks a cloud (e.g. Cloud A), rents the storage space and transfers the information to Cloud A. After the client appreciates the storage benefit for a timeframe, he/she may not fulfill it or find a superior cloud storage benefit. Subsequently, the client leases the storage space gave by another cloud storage supplier (e.g. Cloud B), and moves the outsourced information from Cloud A to Cloud B. To guarantee the information integrity amid these procedures, the client uses a remote information integrity checking convention to confirm the integrity of the cloud information.

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

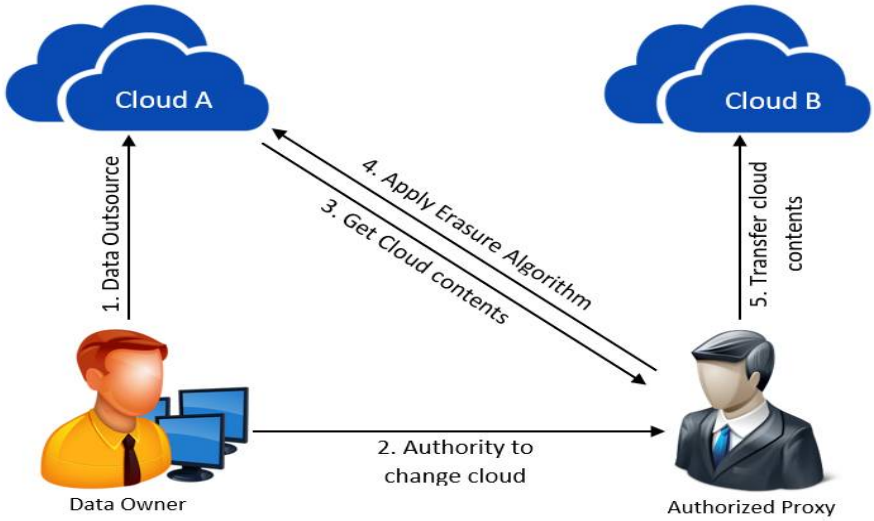


Fig. 1.System Model.

B.SECURITYTHREATS:

Security dangers towards client's outsourced information are from both interior and outside assaults. The outer assailants, for example, spurred programmers, may degenerate the outsourced information when they are keeping up on the cloud servers or transmitting on channels. The interior aggressors, including the legitimate yet inquisitive cloud storage suppliers, may erase the information that are once in a while or never got to on the servers. Specifically, the accompanying security dangers ought to be considered.

• **Data Protection Introduction:** Data confidentiality is a standout amongst the most basic security dangers for clients in cloud storage in the accompanying reasons. Right off the bat, since the cloud servers are keeping up all information, the representatives can wrongfully procure the directors benefits to get to the information by means of framework vulnerabilities. Besides, the clouds may share the keeping up information to their clients or outsource the information to subcontractors. To wrap things up, since the information from various clients are keeping up on the same physical server, a few clients may vindictively read the information of different clients cross the virtual machines. Thusly, the outsourced information are powerless against different dangers in clouds, and every one of the information are presented to general society once they are transferred to the cloud servers.

• **DataDebasement:** Due to the regular information access and refresh tasks, the likelihood of information blunders happen increments and the life time of storage medium turns out to be short. In this manner, the information misfortune mishaps may happen out of the blue and the cloud storage suppliers attempt to shroud these mischances to keep up a decent notoriety. The clouds may likewise erase a few information that are once in a while or never went to lease the spaces to different clients for money related benefits. Also, Cloud A may send a bit of the expected information to Cloud B and claim that every one of the information are exchanged,or send manufactured information to cheat the client.

• **Copy Reservation:** The cloud may save the exchanged information and attempt to find some verifiable benefits from them. This conduct is unforeseen from clients' perspectives. Also, the duplicate reservation may cause the divulgence of the touchy data about clients**.**

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

• **Secure Data Erasure:** There ought to be a successful instrument to guarantee that the duplicates in Cloud are disposed after the data are exchanged to Cloud B. In this manner, the clients have no stresses over the data spillage because of the duplicate reservation in Cloud A.

C. PROPOSED SODT SCHEME

To accomplish the outsourced data confidentiality and integrity verification, the clients scramble their data hinders before transferring them to Cloud A by using the enhanced BCP encryption conspire and process the polynomial-based labels for the data squares. Amid the remote data integrity checking, the clouds can total the ciphertexts of data pieces and the comparing labels to produce a proof with a consistent size to demonstrate the accuracy and integrity of the data.Here we introduce proxy to transfer the data from cloud A to cloud B. Amid the data exchange, the normal Cloud B can confirm the data integrity by methods for clump verification and acknowledge the uncorrupted data. Moreover, to ensure secure data erasure on Cloud A, we utilize the Reed-solomon erasure code method to erase the data for the benefit of Cloud B and dispose of the old decoding key. In this way, the data in Cloud An are undecryptable and no aggressor can recuperate any significant data from these duplicates.

A. REED-SOLOMON ERASURE CODE

Given an original data file, Reed-Solomon erasure code firstly divides it into K fragments of the same size and then encodes them into n fragments. Any K fragments taken out ofthe n encoded ones can be used to reconstruct the original data file. Meanwhile, it is impossible to obtain any information about any fragment of the original data from less than k fragments. Therefore, Reed-Solomon code supports K-resistance and ensures high security. This code is customarily referred to as (n,K) Reed-Solomon code.

Mathematically, (n,K) Reed-Solomon code can be expressed as

$$S=G.F \quad (1)$$

Theorem 1. Let G be a generator matrix of a (n,K) linear Reed-Solomon code. If any K square submatrix of G is invertible, then any K encoded data fragments are sufficient to reconstruct the original data file.

Proof.

Let S* be the row vectors consisting of any K elements of the encoded data file S (i.e., S* is composed of any K encoded data fragments) and G* the corresponding K square submatrix of G.Obviously, we can infer from:

$$S^*=G^*.F \quad (2)$$

From the assumption, since the submatrix G* is linearly independent, then

$$F=(G^*)^{-1}.S^* \quad (3)$$

According to the above equation, the original data file can be reconstructed.

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

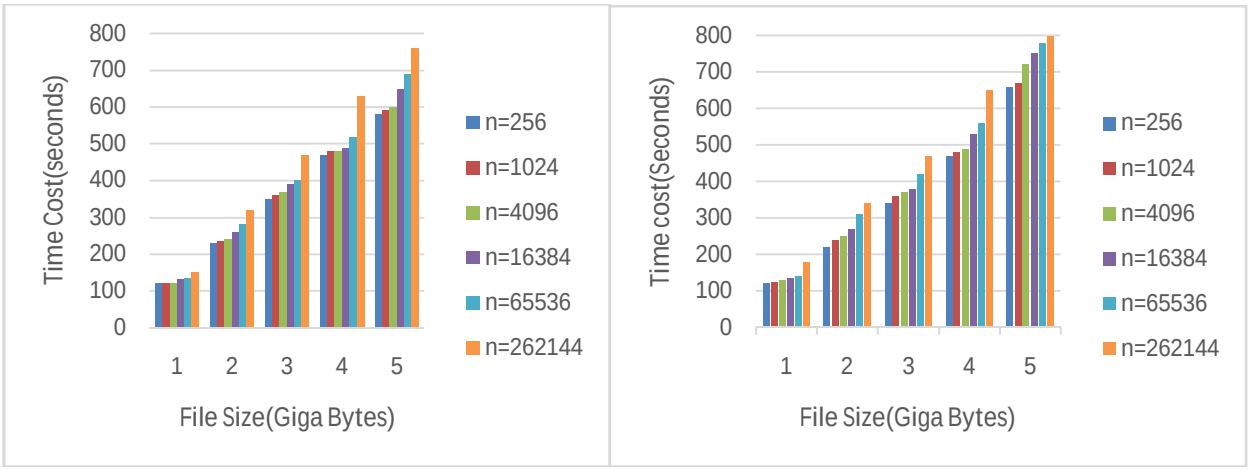
2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

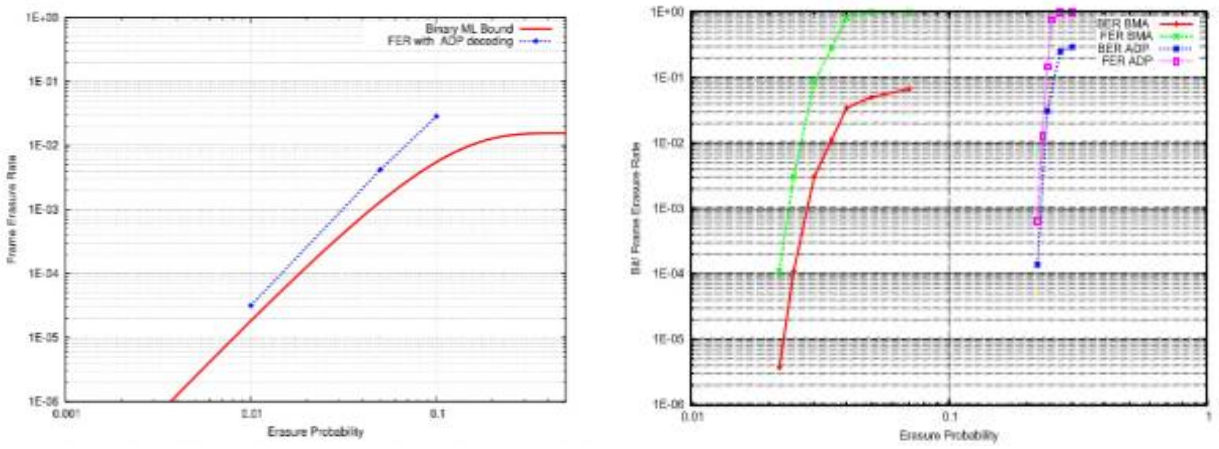
Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

IV. EXPERIMENTAL RESULTS



(a) Time cost for users in store (b) Time cost for cloud in transfer

Fig. 2. computational overhead in store and transfer



(a) Reed – Solomon code compared to ADP (b) Performance of Reed – Solomon compared to BEC

Fig. 3. Performance of Reed – Solomon erasure code

To investigate the computational overhead of SODT, we direct a test on a journal with Intel Core i5-4200U CPU @ 2.29GHz and 4.00GB memory. We utilize the MIRACL library to actualize number-theoretic based techniques for cryptography. The RSA modulus N is roughly 1024 bits and the parameters p and q are both 512 bits. In Fig. 2(a), we demonstrate the execution time of clients to process a file with the measure of 1GB, 2GB, 3GB, 4GB or 5GB in Store stage, and each file is partitioned in 262144, 65536, 16384, 4096, 1024 or 256 pieces, separately. Fig. 2(b) demonstrates the running time of the cloud to get the comparing relocating file from another cloud in that the security

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

of our proposed conspire relies upon the numerically difficult issues. At long last, we have exhibited the efficiency of our plan by directing an investigation. For the future work, we will outline a secure data exchange conspire with fine-picked up data sharing for cloud storage.

On the off chance that the quantity of pieces is substantial than 16384, the execution time of clients in Store and mists in Transfer increments significantly. In Fig. 2, we set c = 300 and c = 460, and exhibit the time cost of the cloud while producing the verification to react the respectability challenge, and the clients that check the legitimacy of the confirmation in Integrity Check stage. In the event that the quantity of divisions is under 16384, the calculations of the cloud to produce the verification are not tedious. The time cost of clients to check the verification is essentially connected with the quantity of tested squares. The correspondence overhead is moderately low for our plan. Specifically, to accomplish secure information exchange, the proxy apply's an intermediatory erasure code known as Reed- Solomon erasure code for secure information exchange between the clouds. As we can see in Fig. 3 the proposed Reed - Solomon code has better performance than the other erasure algorithms.

V. CONCLUSION

In this paper, we have proposed a secure outsourced data exchange plan to ensure the clients' outsourced data when they are exchanging from one cloud to another one. In the proposed plot, we have built up an upgraded BCP encryption to encode the clients' data to keep the touchy data from being unveiled, and the polynomial-based authenticators to accomplish efficient remote data integrity verification. we also propose the data erasure model in the clouds with the help of proxy who takes the data from the cloud and transfer it to another and ensure that the previous data is being erased and the owners data integrity is maintained.The intermediary re-encryption method is utilized to securely and sufficiently dispose of the moved data in cloud. We have additionally examined the security properties and demonstrated.

REFERENCES

[1] "Secure Outsourced Data Transfer with Integrity Verification in Cloud Storage" Jianbing Ni, Xiaodong Lin, Kuan Zhang, Yong Yu, and Xuemin (Sherman) Shen.
[2] H. Li, Y. Yang, X. Liang, T.H. Luan, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified subdictionaries over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, to apprear.
[3] Cisco, "Cisco global cloud index: forecast and methodology, 2013– 2018," Cisco GCI White Paper, 2014.
[4] A.Chang,"7criticalcloudserviceattributes,"InformationweekNetwork Computing, 2014.
[5] K. Yang, Z. Liu, X. Jia, and X. Shen, "Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach," IEEE Transactions on Multimedia, to appear.
[6] C. Wang, K. Ren, W. Lou, and J. Li, "Toward public auditable secure cloud data storage services," IEEE Network, vol. 24, no. 4, pp. 19–24, 2010.
[7] Cloud Security Alliance, "Top threats to cloud computing," http://www.cloudsecurityalliance.org, 2010.
[8] H. Li, D. Liu, Y. Dai, T.H. Luan, and X. Shen, "Enabling dfficientmultikeyword ranked search over encrypted mobile cloud sata through blind storage," IEEE Transactions on Emerging Topics in Computing, vol.3, no.1, pp. 127–138, 2015..
[9] L.M. Kaufman, "Data security in the world of cloud computing," IEEE Security & Privacy, vol. 7, no. 4, pp. 61–64, 2009.
[10] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.
[11] J. Ni, Y. Yu, Y. Mu, and Q. Xia, "On the security of an efficient dynamic auditing protocol in cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 10, pp. 2760–2761, 2015.
[12] J. Reardon, H. Ritzdorf, D. Basin, and S. Capkun, "Secure Data Deletion from Persistent Media," in Proc. of ACM CCS 2013, Berlin, Germany, 2013, pp. 271–283.
[13] F. Hao, D. Clarke, and A. Zorzo, "Deleting secret data with public verifiability," IEEE Transactions on Dependable and Secure Computing, to appear.
[14] Cloudsfer, "Migrate & backup your files from any cloud to any cloud," http://www.cloudsfer.com/#oht:lang=en-us, 2015.
[15] Y.Yu, J. Ni, W. Wu, and Y. Wang, "Provable data possession supporting secure data transfer for cloud storage," in Proc. of BWCCA 2015, Ploand, 2015, pp, 38–42.
[16] H.Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Sydney, Australia, 2008, pp. 90-107.