RESEARCH ARTICLE OPEN ACCESS

EDLC: Enhanced Data Leakage Controller for Secure Multi-Cloud Storage

Mr. Arvind Dalvi

PG student, Computer Department, JSPM's JSCOE, Handewadi, Pune.

Prof. Satav S. D.

IT Department, JSPM's JSCOE, Handewadi, Pune.

----------**********----------

Abstract:

Multiple Cloud storage has become one of the essential services of cloud computing. This Multi Cloud storage models permit users to store sliced encrypted knowledge in numerous cloud drives. Thus, it provides support for various cloud storage services using the single interface rather than using single cloud storage services. Cloud security goal primarily focuses on issues that relate to info privacy and security aspects of cloud computing. Cloud computing is nothing however rate server and web based mostly model .A huge quantity of knowledge being retrieved from geographically distributed information sources and non-localized information handling needs. It provides support for varied cloud storage services exploitation the single interface rather than exploitation single cloud storage services. Cloud security goal primarily focuses on problems that relate to data privacy and security aspects of cloud computing. This latest information storage service and information moderation prototype focus on malicious insider's access on keep information, protection from malicious files, removal of centralized distribution of information storage and removal of obsolete files or downloaded files oftentimes. Information owner will not essentially need to worry concerning the future of the information keep in the Multi - Cloud server is also extracted or depraved. the opposite is ingress control of information. The projected technique ensures the file or information cannot get access while not the data or permission of the owner. Thus, this analysis aims at offering associate degree design that reduces malicious insiders associate degreed file threats with an formula that improves information sharing security in Multi - Cloud storage services. This technique can supply a secure atmosphere whereby the information owner will store and retrieve data from Multi - Cloud Environment while not file merging conflicts and prevents corporate executive attacks to get meaningful information. The experimental results indicate that the instructed model is appropriate for call making method for the information house owners in the better adoption of multi - cloud storage service for sharing their data securely

Keywords —**Multi-Cloud storage, Enhanced Data Leakage Controller.**

----------**********----------

I. INTRODUCTION

Multi Cloud is the utilization of various computing services in a single heterogeneous architecture. Multi Cloud Storage means the utilization of various cloud storage services using a single web interface rather than the defaults provided by the cloud storage vendors in a single heterogeneous architecture. Multi Cloud data systems have the capacity to enhance data sharing and this aspect will be significantly of great help to data users. It enables data owners to share their data in the cloud. In any cloud computing model, security is thought to be the foremost crucial side thanks to the sensitivity and delicacy of the user's data or knowledge hold on in a very cloud. Presently, each Organization is pushing its IT department to proportion their knowledge sharing systems. Most cloud services don't seem to be free and possess completely different sizes. For instance, Single Cloud Storage falls among the services with storage limitation that makes it minus compared to multi-cloud storage. The main advantage of using multi cloud storage is performance and higher security for data sharing. In the single cloud storage knowledge remains on the centralized storage which may be simply accessed by the malicious insiders. Companies ought to get thinking about operating with quite one cloud supplier at a time -for price savings, performance, disaster recovery and other reasons. Most business organizations share most of their knowledge with either their shoppers or suppliers and take into account knowledge sharing as a priority. Cloud providers are offering efficient on-demand storage solutions that can virtually scale indefinitely. Many public cloud storage providers are already available in the market, such as Amazon S3 (http://aws.amazon.com/s3), Google Storage (http://code.google.com/apis/storage), Microsoft Azure (http:// microsoft.com/windows azure) or Rack Space Cloud Files (http://rackspace.com/cloud) and one may expect new providers to appear in the coming years. The offers in terms of pricing among providers vary significantly and may change over time to adapt to the market. Choosing the best-suited or cheapest provider for your data implies knowing in advance the access pattern to the data. Data that is rarely accessed should be stored at a cloud provider mainly with a low storage price, regardless of its access prices. On the other hand, a very popular data may be hosted on a provider with attractive price for the outgoing bandwidth. In most cases, it is difficult to know in advance the access pattern of a data item, and therefore one needs an adaptive solution to choose the most cost-efficient provider. However, finding a suitable provider based on the access pattern of the data is not enough. A provider may end its business or suddenly increase its pricing policy. There exist many other technical as well as non-technical (e.g., boycotting a provider) reasons a user may want to change its provider. Therefore, in order to safely host its data and minimize the partially supported by the EU project Open IoT. impact of the migration to a new provider, a user needs to proactively avoid vendor lock-in (i.e., being dependent on a specific service vendor with substantial switching costs) and ensure high durability and availability by geographic diversification of the data placement (e.g., the recent Amazon outage reminds us not to put all eggs in one basket.

The integrity and confidentiality of data and services are related with access control and identity management. It is important to maintain track record for user identity for avoiding unauthorized access to the stored data. The identity and access controls are complex in cloud computing because of that data owner and stored data are at different executive platforms. In cloud environment, different organizations use variety of authentication

authorization agenda. By using different approaches for authentication and authorization gives a compound situation over a period of time. The cloud resources are dynamic and are elastic for cloud user and IP addresses are continuously changed when services are started or restarted in pay per usage model. That allows the cloud users to join and leave feature to cloud resources when they required i.e., on-demand access policy. All these features need efficient and effective access control and identity management. The cloud has to maintain quickly updating and managing identity management for joining and leaving users over cloud resources. There are many issues in access control and identity management, for example weak credentials may reset easily, denial of service attack to lock the account for a period of time, Weak logging and monitoring abilities, and XML wrapping attacks on web pages.

Data loss, which suggests a loss of information that occur on any device that stores data. It might be problem for anyone that uses a computer. Data loss occurs when data may be physically or logically removed from the organization either intentionally or unintentionally. The data loss has become a main problem in organization today where the organizations are in responsibility to overcome this problem. Data Leakage happens when the confidentiality of information has been compromised. It shows an unauthorized transmission of data from within an organization to an external destination. The data that is leaked out can either be non-public in nature and area unit deemed confidential whereas knowledge Loss is loss of knowledge because of deletion, system crash etc. Totally both the term can be referred as knowledge breach, has been one in every of the biggest fears that organization face today. The advantages brought by this new registering model incorporate yet are not restricted to: help of the weight for capacity the board, all-inclusive information access with autonomous topographical areas, and evasion of capital consumption on equipment, programming, and work force systems for upkeeps, and so on. With the pervasiveness of cloud administrations, increasingly more touchy data are being brought together into the cloud servers, for example, messages, private recordings and photographs, organization fund information, government records, and so on. At first glance, distributed storage has a few points of interest over conventional information capacity. For instance, in the event that you store your information on a distributed storage framework, you'll have the capacity to get to that information from any area that has Internet get to.

You wouldn't have to bear a physical capacity gadget or utilize a similar PC to spare and retrieve your data. As information proprietors store their information on outer servers, there have been expanding requests and worries for information privacy, validation and access control. Information is greatest resource for an association and how classification, authentication and access control can be re-appropriated. There is a danger to information proprietor that if CSP is malignant or CSP has some weakness. Henceforth information proprietor must have some method for guaranteeing the information is classified from CSP

II. Related Work

Protection and security for disseminated stockpiling are all around a wide region of research. Different insightful rounds of questioning have been directed to perceive the potential security issues about this subject. Note that sharing records over cloud stage have various vulnerabilities that can prompt unapproved get to. The aggressors of cloud have fluctuated intensions or objectives which lead to the poor picture of the cloud suppliers once the objective is accomplished [1].

In the perspective of [2] design has been proposed for sharing medicinal services records in multi-distributed storage utilizing Attribute Based Encryption (ABE) and cryptographic mystery sharing. Multi-Cloud mediator parts the encoded record and stores it in the Multi-Cloud. The primary downside in this methodologies are amass sharing requires gigantic calculation and long holding up time, since document ordering isn't utilized questionable data results in record recovery process. Since the CP-ABE is given by outsider malignant insider may have simple access to the information. Document measure in excess of 50 MBs increment the client's holding up time. The investigations are performed utilizing an exceptionally arranged machine subsequently it is cost expending progressively. Vindictive documents are additionally effortlessly transferred by the outsider expert or job based administrators to degenerate the whole plan. Every one of the undertakings are not computerized i.e. to transfer a document customer must make a marked restorative record utilizing CP-ABE Scheme. Cloud supplier's parts the information and exchanges information from multi-cloud intermediary to cloud information sources.

So as to upgrade the protected information partaking in the multi-distributed storage [3] proposed design with an Advanced Encryption Standard Algorithm (AES) which looks to give better distributed storage basic leadership for the clients. Yet, insider assaults, conniving assaults, information uprightness, information get crasher and malignant documents have not been engaged.

To shield the information from pernicious insiders [4] presented a Secure Data Sharing in Clouds approach which utilizes outsider server to store a piece of the encryption key and other part is kept up by the client. On the off chance that the denied client and outsider server plots information can be recovered from the cloud. So also if the vindictive cloud administrator and outsider server conspires information can be recovered. This technique utilizes single distributed storage and henceforth brought together appropriation of delicate information isn't suggested for the clients. Bigger documents of 100 MB decrease the execution of this strategy and makes client to hang tight for a more extended time since transferring and encryption process are done successively.

In [5], an intermediary re-encryption conspire for secure information partaking in cloud however private key gets completely uncovered when renounced client and intermediary connives. Moreover the whole record is put away in single distributed storage which has low security and productivity. The remaking of information from multi-cloud requires a compelling technique to consolidate every one of the documents without changing the significant data.

In [6] especially comparable methodology has been proposed yet does not ensure the security for Meta table and neglected to encode the video and other huge documents. When the Meta table data is lost, recovery process will be a dreary work.

In [7] Secure Scalable and Efficient Multi-proprietor information sharing plan has been proposed. This plan coordinates Identity Based Encryption and hilter kilter assemble consent to empower gather situated access control for information proprietors in a many-to-many sharing example. Anyway the key age process is done by the outsider as a different procedure and encryption and decoding process is done as another procedure which is weight to the information proprietor to sit tight for the culmination of the entire procedure. Noxious records assurance has not been ensured. Unified appropriation of information stockpiling has not been much encouraging to the clients to share their information. Character based encryption

underpins just little information of 50MB. Enter escrow issue emerges in Identity based plan.

Crafted by [8] presented a safe document partaking in multi-cloud utilizing Shamir's mystery sharing plan and base 64 encoding in their calculation. Vindictive insider's assaults have been anticipated by this plan. Regardless, requesting of reports has not been used so that in the recuperation methodology recipient needs to pick all of the offers to encode and imitate the record which is load to the gatherer. Likewise vindictive records are not forestalled and robotization of the considerable number of errands in this plan has not been engaged which decreases the general effectiveness of this plan. Numerous comparative methodologies has been proposed yet neglected to actualize a successful design and working technique for the safe information sharing utilizing the Multi Cloud stockpiling suppliers. The current above methodologies does not ensure the robotization of document cutting, encryption, unscrambling and recovery process. Existing exploration likewise does not concentrate on the combining document clashes in the recovery procedure, malevolent records, plotting supplier assaults, insider assaults, expulsion of unified appropriation of information and key administration while sharing the information in Multi-Cloud Storage. Additionally all the current designs of single distributed storage and Multi-Cloud Storage pursues a similar example that is record transferring, encryption and cutting without list. On the off chance that an encryption procedure is done before cutting vast documents or video records can't be transferred safely and what's more it might likewise result to hang tight the client for a more drawn out time. Vindictive records can in like manner be viably exchanged which makes hurts the multi cloud server in the present philosophies.

Support Malicious reports [9] are recognized in provider's condition or by using untouchables basically after mischief is caused. The proposed presentation is arranged in such a way when the malicious record gets exchanged it first impacts the proprietor's machine.

In this paper [10], they proposed an anchored financially savvy multicloud capacity (SCMCS) in distributed computing, which tries to give every client a superior cloud information stockpiling choice, thinking about the client spending plan and also furnishing with the best nature of administration. The model has demonstrated its capacity of giving a client an anchored stockpiling under his moderate spending plan. It gives a better decision than customers as shown by their available spending designs. In that demonstrate, the client isolates his information among a few SPs accessible in the market, in view of his accessible spending plan.

The expanding prominence of distributed storage administrations has lead organizations that handle basic information to consider utilizing these administrations for their capacity needs. Therapeutic record databases, control framework recorded data and budgetary information are a few instances of basic information that could be moved to the cloud. Nonetheless, the unwavering quality and security of information put away in the cloud still stay real concerns. In this paper we present DEPSKY, a framework that enhances the accessibility, respectability furthermore, classification of data put away in the cloud through the encryption, encoding and replication of the information on different mists that frame billow of-mists [11].

we investigated end-clients' security desires what's more, suppositions about distributed storage, and additionally their mindfulness of dangers, terms and conditions. We directed 36 indepth meets in Switzerland and India, and followed up with an

online study with 402 members. Our outcomes propose that clients make overwhelming utilization of free webmail accounts as distributed storage drives. Be that as it may, rather than depending on the cloud as a principle stockpiling unit, clients keep nearby reinforcements of cloud-put away information [12].

We blessing NCCloud, a different distributed storage documenting framework that much tends to the reliableness of the present distributed storage. NCCloud not exclusively accomplishes adaptation to non-critical failure of capacity, anyway furthermore allows cost-productive fix once a cloud for good falls flat. NCCloud actualizes a sensible form of the viable least stockpiling make code (F-MSR), that recovers new lumps all through fix subject to the predefined level of information excess. Our NCCloud embodiment demonstrates the viability of FMSR in getting to data, regarding monetary costs and reaction times [13].

Despite the fact that the quantity of distributed storage administrations accessible over the world keeps on expanding, the onus is on application designers to imitate information over these administrations. We create SPANStore to send out a brought together perspective of topographically circulated capacity administrations to applications and to computerize the way toward exchanging off expense and idleness, while fulfilling consistency and adaptation to non-critical failure necessities [14].

In this paper we exhibited a procedure to check both capacities and framework structure of individual distributed storage ser- indecencies. We at that point assessed the ramifications of plan decisions on execution by examining 5 administrations. Our investigation demonstrates the importance of customer capacities and convention structure to individual distributed storage administrations. Dropbox executes a large portion of the checked abilities, and its so- phisticated customer obviously helps execution, albeit a few convention changes appear to be conceivable to lessen organize overhead [15].

To the best of our insight, we are the first to break down the utilization of Dropbox on the Internet. Our examination surveyed the expanding enthusiasm on cloud-based capacity frameworks. Significant players like Google, Apple and Microsoft are putting forth the administration. We demonstrated that, in this scene, Dropbox is right now the most prevalent supplier of such a framework. Dropbox is at this point in charge of an impressive traffic volume. In one of our datasets, for example, Dropbox is as of now proportionate to 33% of the YouTube traffic [16].

III. PROPOSED ALGORITHM

A. *Description of the Proposed Algorithm:*

1) Register & Login

- In this module, data owner and data user register with EDLC based on his username, password, name, mobile no, and so on.
- Followed by, both are login and access file upload & download process in multi cloud neutral.

2) Encrypt & Upload:

- In this module, a data owner wants to upload his files to Multi-cloud. So he sends the upload request to EDLC.
- After receiving the upload request, the EDLC generates public key and private key for each upload request.
- Then split a file into chunks and encrypt each chunk. At the same time, it generates HMACSHA1 signature for each encrypted chunks.
- Then upload all encrypted chunks with signatures to multi-cloud.

3) Download & Decrypt:

- In this module, a data owner wants to download his files from multi-cloud. So he sends the download request to EDLC.

- After receiving the download request, the EDLC download all encrypted chunks from multi-cloud. Then generates new HMACSHA1 signature for each encrypted chunks

- Then checks new signature is equal or not with old signature. If both signatures are same it considers encrypted chunk is safe. Otherwise leaked.

- After signature verification, it decrypts all encrypted chunks based on private key. Followed by, it merges all chunks and forward to data owner.

IV. PSEUDO CODE

Data Owner:

Step 1) Register
Step 2) Login
Step 3) Symmetric Key (AES), Secret Key (DES), Public and Private Key Generation
Step 4) Uploads file
Step 5) Calculate size of the file.
Step 6) Split or Divide the file into Blocks based on the service providers integrated with Multi Cloud.
Step 7) Each part of the file is encrypted and uploaded to the multicloud environment.

Data User:

Step 1) Register
Step 2) Login
Step 3) Get the File Name (FN) and Secret Key (SK) from the data owner or File owner by making request to the processor
Step 4) Enter or Pass that File Name (FN) and secret Key (SK). Perform a search with the filename associated in each Multi Cloud storage service provider directory (F.0, F.1, F.2, F.3 and F.4) and obtain the path of the encrypted files E (F.1), E (F.2), E (F.3), E (F.4) and E (F.5)
Step 5) Pass the user defined secret key (SK) to the Unicode Encoding Object to initialize a key (K) and a vector (V) which can be used to create symmetric Decrypt or object
Step 6) Merge each part of the decrypted files F1, F2, F3, F4, and F5 from Multi Cloud storage service provider to obtain the original file F. Auto removal of all decrypted and encrypted parts of the files stored in the respective services.

V. SIMULATION RESULTS

This work proposed an Enhanced Data Leakage Controller (EDLC) which decreases pernicious insiders and information spillages with a calculation that enhances information sharing security in Multi-Cloud stockpiling administrations. This proposed work gives security against the two information spillage and information changes. The EDLC ensures the record cutting with list based parts gets encoded and put away on the Multi-Cloud. After receiving the upload request, the EDLC split a file into chunks and encrypt each chunk. At the same time, it generates HMACSHA1 signature for each encrypted chunks.
After receiving the download request, the EDLC download all encrypted chunks from multi-cloud. Then generate new HMACSHA1 signature for each encrypted chunks. It checks new signature is equal or not with old signature. If yes then only consider chunk is safe. This strategy will offer a safe situation whereby the information proprietor can store and recover information from Multi-Cloud Environment.

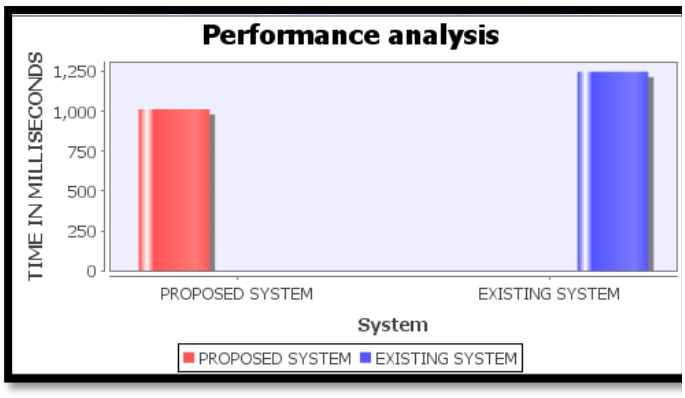

Fig.1. Performance analysis for 1 MB file

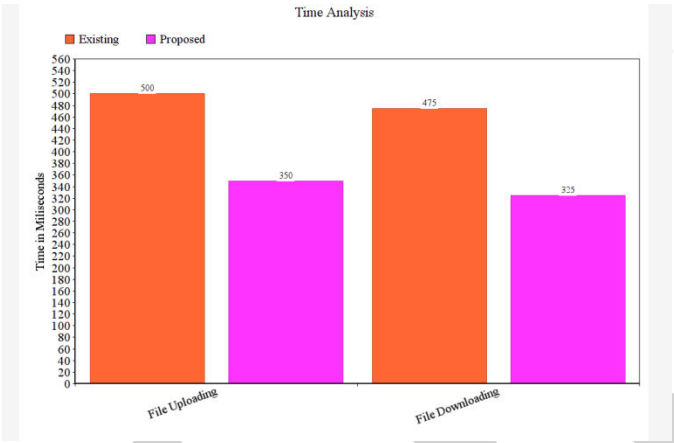

Fig.2. Time analysis of Existing and Proposed system

In figure 2, time analysis of the existing and proposed system is shown in which file uploading and file downloading time is shown, which shows time required for existing system is more as compared to proposed system.

VI. CONCLUSION AND FUTURE WORK

We addressed the problem of methods provide a user-specific weight for each cloud which only coordinates the fraction of storage load for each cloud but cannot prevents the information leakage across the CSPs efficiently. So Distributing data on multiple clouds provides users with a certain degree of information leakage control in that no single cloud provider is privacy to the entire user's data. Distributing data on multiple clouds provides users with a certain degree of information leakage control in that no single cloud provider is privacy to the entire user's data. However, unplanned distribution of data chunks can lead to avoidable information leakage. To tackle this problem, this work proposed an Enhanced Data Leakage Controller (EDLC). It controls information leakage efficiently

REFERENCES

[1] Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo "*Secure Data Sharing in the Cloud*". In Security, Privacy and Trust in Cloud Systems, Springer Berlin Heidelberg, 2015, (pp. 45-72).

[2] Benjamin Fabian, Tatiana Ermakova, Philipp Junghanns "*Collaborative and secure sharing of healthcare data in multi-clouds*", Information Systems, Volume 48 Issues C, 2015, pp 132-150

[3] Balasaraswathi, V. R., &Manikandan, S. (2014)," *Enhanced security for multi-cloud storage using cryptographic data splitting with dynamic approach*", In Advanced Communication, International Conference on Control and Computing Technologies (ICACCCT), 2014 on (pp. 1190-1194) IEEE.

[4] Mazhar Ali, Revathi Dhamotharan, ErajKhan, Samee U. Khan, Athanasios V. Vasilakos, KeqinLi, Albert. Y. Zomaya "*SeDaSC: Secure Data Sharing in Clouds*", Systems Journal, IEEE, volume: PP, Issue: 99, 2015, pp 1-10.

[5] Wang Liang-liang, Chen Ke-fei, Mao Xian-ping, Wang Yong-tao "*Efficient and Provably-Secure Certificate less Proxy Re-encryption Scheme for Secure Cloud Data Sharing*" Journal of Shanghai Jiaotong University Volume 19, issue 4,2014 pp 398-405.

[6] Peng Xu, Xiaqi Liu, Zhenguo Sheng, Xuan Shan, Kai Shuang "*SSDS-MC: Slice-based Secure Data Storage in Multi-Cloud Environment*" 11th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE), 2015,pp 304-309.

[7] Shungan Zhou, Ruiying Du, Jing Chen, Hua Deng, Jian Shen, Huanguo Zhang "*SSEM: Secure, Scalable and Efficient multi-owner data sharing in clouds*", China Communications IEEE ,Volume 13,issue 8, 2016,pp 231-243.

[8] Ibrahim Abdullah Althamary, Talal Mousa Alkharobi "*Secure File Sharing in Multi-Cloud using Shamir's*

Secret Sharing Scheme", Transactions on Network and communications Vol 4 issue 6, 2016,pp53-67.

[9] Safaa Salam Hatem, Maged H.Wafy,Mahmoud M.EI-Khouly "*Malware Detection in cloud Computing*",International Journal of Advanced Science and Computer Science Applications,Vol 5 No 2014.

[10] Yashaswi Singh, Farah Kandah, Weiyi Zhang, "*A Secured Cost-effective Multi-Cloud Storage in Cloud Computing*," IEEE INFOCOM on Cloud Computing in 2011.

[11] Thanasis G. Papaioannou, Nicolas Bonvin and Karl Aberer, "*Scalia: An Adaptive Scheme for Efficient Multi-Cloud Storage*," IEEE November 10-16, 2012.

[12] Emil Stefanov and Elaine Shi, "*Multi-Cloud Oblivious Storage*," IEEE ACM 978-1-4503-2477, November 4–8, 2013.

[13] Rohit Bhadauria, Rituparna Chaki, Nabendu Chaki and Sugata Sanyal, "*A Survey on Security Issues in Cloud Computing*," Journal of Network and Computer Applications Volume 71, August 2016.

[14] Shilpashree Srinivasamurthy and David Q. Liu, "*Survey on Cloud Computing Security*," IEEE International Conference on Computing Sciences on 24 December 2012.

[15] Marina Zapater, Jos´e L. Ayala, Jos´e M. Moya, Kalyan Vaidyanathan, "*Leakage and Temperature Aware Server Control for Improving Energy Efficiency in Data Centers*," IEEE Conference 06 May 2013.

[16] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, And Ninja Marnau, "*Security And Privacy-Enhancing Multicloud Architectures*," IEEE Transactions On Dependable And Secure Computing, Vol. 10, No. 4, July/August 2013.

[17] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma, "*Cloud Computing Security - Trends and Research Directions*," IEEE World Congress on Services 4-9 July 2011.