IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10328

Multicloud Storage with Enhanced Security in Cloud Environment

Ms. Amruta Vedpathak[1], Prof. V. V. Pottigar[2]

Punyashlok Ahilyadevi Holkar Solapur University, Solapur[1]

Department of Computer Science & Engineering, NBNSCOE, Solapur[2]

Abstract: Multi-Cloud Storage infers the use of varied appropriated stockpiling organizations employing a singular web interface instead of the defaults given by the circulated stockpiling shippers during a single heterogeneous plan. This Multi-Cloud accumulating model empowers customers to store cut mixed data in various cloud drives. Right now, offers assistance for various appropriated stockpiling organizations using the only interface as against using single circulated stockpiling organizations. Cloud security objective basically focuses on issues that relate to information insurance and security parts of dispersed processing. Likewise, the info in clients' information is often spilled e.g., by methods for malignant insiders, indirect accesses, pay off and pressure. This latest data accumulating organization and data control model specialise in vindictive insider's passageway on put aside data, affirmation from malignant archives, removal of united dissemination of knowledge storing and clearing of out of date records or downloaded records once during a while. Data owner doesn't generally got to worry over the destiny of the info put aside within the Multi-Cloud server could also be removed or ruined. The opposite is entrance control of knowledge. The exploratory results exhibit that the suggested show is suitable for essential authority process for the info owners within the more sensible choice of multi-disseminated capacity advantage for sharing their information securely.

Keywords: Multicloud storage, information leakage, system attackability ,remote synchronization, distribution and optimization

I. INTRODUCTION

Multi-Cloud is that the usage of various registering administrations during a solitary heterogeneous design. Multi-Cloud data structures can update data sharing and this viewpoint are going to be through and thru of wonderful assistance to data customers. It empowers information proprietors to share their information within the cloud. In any distributed computing model, security is viewed because the most pivotal angle due to the affectability and delicacy of the client's data or information put away during a cloud. By and by, each Organization is pushing its IT office to proportion their information sharing frameworks. Most cloud administrations aren't free and have various sizes. For instance, Single Cloud Storage falls among the administrations with capacity constraint which makes it disadvantageous in contrast with multi-distributed storage. The first superiority of utilizing multi distributed storage is execution and better security for information sharing. Within the single distributed storage information stays on the unified stockpiling which may be effectively gotten to by the vindictive insiders. Associations should get thinking about working with quite one cloud provider without a moment's delay - for cost speculation reserves, execution, disaster recovery and various reasons. Most business affiliations share a huge segment of their data with either their clients or suppliers and consider data sharing as a requirement [1]. Through information sharing, higher efficiency levels are come to. With a couple of clients from different associations adding to the cloud information, cost and time spent would be less contrasted with the customary methods for physically sending and sharing information, which regularly prompted the assembly of obsolete and excess reports [1]. Albeit numerous cryptographic information cutting strategies [2], [3], [4] are proposed because the principle issue emerges within the insider's entrance to place away information. Insiders are the confided in optional administrator or supervisors who continue the outsider server with an identical approval because the administrator. Since the outsider servers or framework has been utilized to store any delicate data.

Heads and outsiders affect the inspiration as they need remote access to the servers; within the event that overseers or outsider directors are pernicious, at that time they access the client's information. The opposite risk isn't normal for the only distributed storage; recovery of the cut documents from the multi-cloud server isn't an easy system. Also, malevolent records are often effectively transferred altogether the present methodologies in single distributed storage and multi-distributed storage. The lesser center has been applied in structuring the multi cloud design when pernicious documents are transferred. The most existed arrangement is that the coordination antivirus apparatus from the outsider or cloud supplier which makes client to hold tight for a more drawn out time while transferring the records. Circulating information over various distributed storage suppliers (CSPs) naturally furnishes clients with a selected level of

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10328

knowledge spillage control, for no single purpose of assault can release all the info. Regardless, off the cuff dispersal of knowledge pieces can incite high information introduction even while using various fogs. To manage this issue, this work proposed an Enhanced Data Leakage Controller.

This proposed work gives protection from the 2 information spillage and knowledge alterations. The EDLC ensures the record cutting with file based parts gets scrambled and put away on the Multi-Cloud. This system guarantees the record can't get access without the knowledge or authorization of the proprietor. Information proprietor transfers the document through the proposed system interface. The system transfers the record within the neighbourhood machine. The system parts the record with its files appointed and scrambles each bit of the document utilizing the mystery or private key gave by the proprietor. Each bit of the scrambled document gets put away within the proprietor's machine and afterward moved to the multi-cloud server. The recipient sends the unscrambling solicitation to the proprietor or the proprietor can share the required accreditations through Bring Your Own Secure Channel (BYOC) or out of band strategy. The beneficiary enters the accreditations through the structure interface. The structure recover the document parts and each part get unscrambled, blended and put away the beneficiary's machine.

II. Related Work

Assurance and security for dispersed capacity are all around a good domain of research. Different insightful rounds of questioning are directed to perceive the potential security issues about this subject. Note that sharing documents over cloud stage have various vulnerabilities which will prompt unapproved get to. The assailants of cloud have changed intensions or objectives which cause the poor picture of the cloud suppliers once the target is accomplished [1].

In the perspective on [2] engineering has been proposed for sharing human services records in multi-distributed storage utilizing Attribute Based Encryption (ABE) and cryptographic mystery sharing. Multi-Cloud go-between parts the encoded record and stores it within the Multi-Cloud. The principle disadvantage immediately bunch sharing requires immense calculation and long holding up time, since document ordering isn't utilized vague data brings about record recovery process. Since the CP-ABE is given by outsider noxious insider may have simple access to the knowledge. Document size in more than 50 MBs increment the client's holding up time. The examinations are performed utilizing an exceptionally arranged machine consequently its cost expending continuously. Malevolent records are additionally handily transferred by the outsider position or job based administrators to degenerate the entire plan. All the assignments aren't computerized for instance to transfer a document customer must make a marked clinical record utilizing CP-ABE Scheme. Cloud supplier's parts the knowledge and moves information from multi-cloud intermediary to cloud information sources.

So as to improve 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 dynamic for the clients. However, insider assaults, conspiring assaults, information honesty, information gate crasher and vindictive records have not been engaged.

To shield the information from malignant insiders [4] presented a Secure Data Sharing in Clouds system 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 conspires information can be recovered from the cloud. So also if the vindictive cloud administrator and outsider server intrigues information can be recovered. This technique utilizes single distributed storage and henceforth brought together dispersion of delicate information isn't suggested for the clients. Bigger records of 100 MB lessen the exhibition of this strategy and makes client to sit tight for a more drawn out time since transferring and encryption process are done sequentially.

In [5], an intermediary re-encryption plot for secure information partaking in cloud however private key gets completely uncovered when disavowed client and intermediary intrigues. Moreover the whole record is put away in single distributed storage which has low security and proficiency. The reproduction of information from multi-cloud requires a powerful strategy to combine all the records without changing the significant data.

In [6] especially comparative methodology has been proposed however doesn't ensure the security for Meta table and neglected to encode the video and other enormous documents. When the Meta table data is lost, recovery procedure will be a dull work.

In [7] Secure Scalable and Efficient Multi-proprietor information sharing plan has been proposed. This plan incorporates Identity Based Encryption and unbalanced gathering consent to empower bunch arranged access control

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10328

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 unscrambling process is done as another procedure which is weight to the information proprietor to sit tight for the fulfilment of the entire procedure. Malignant records security has not been ensured. Brought together conveyance of information stockpiling has not been a lot of promising to the clients to share their information. Personality based encryption underpins just little information of 50MB. Key escrow issue emerges in Identity based plan.

Crafted by [8] presented a protected document partaking in multi-cloud utilizing Shamir's mystery sharing plan and base 64 encoding in their calculation. Pernicious insider's assaults have been forestalled by this plan. Regardless, requesting of reports has not been used so that in the recuperation method recipient needs to pick all of the ideas to encode and recreate the record which is weight to the authority. Also noxious records are not forestalled and mechanization of the considerable number of errands right now not been engaged which decreases the general effectiveness of this plan. Numerous comparative methodologies has been proposed however neglected to actualize a powerful design and working methodology for the protected information sharing utilizing the Multi Cloud stockpiling suppliers. The current above methodologies doesn't ensure the mechanization of document cutting, encryption, unscrambling and recovery process. Existing exploration additionally doesn't concentrate on the combining document clashes in the recovery procedure, vindictive records, conspiring supplier assaults, insider assaults, evacuation of brought together circulation of information and key administration while sharing the information in Multi-Cloud Storage. Likewise all the current designs of single distributed storage and Multi-Cloud Storage follows a similar example that is document transferring, encryption and cutting without file. On the off chance that an encryption procedure is done before cutting enormous 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 extended time. Noxious records can in like manner be successfully moved which makes hurts the multi cloud server in the present techniques.

Encourage Malicious documents [9] are distinguished in suppliers condition or by utilizing outsiders simply after harm is caused. The proposed display is planned in such a way when the malevolent records gets transferred it first influences the proprietor's machine.

III. MULTI –CLOUD STORAGE

Right now, they proposed a made sure about financially savvy multicloud capacity (SCMCS) in distributed computing, which looks to furnish every client with a superior cloud information stockpiling choice, contemplating the client spending plan just as furnishing with the best nature of administration. The model has indicated its capacity of giving a client a made sure about capacity under his moderate spending plan. It gives a better decision than customers as demonstrated by their open spending plans. In that model, the client isolates his information among a few SPs accessible in the market, in view of his accessible spending plan.

They introduced Scalia [11], a framework that consistently enhances the situation of information put away at different cloud suppliers, in light of their entrance insights. We depicted in detail the different layers of our methodology and our versatile instrument for versatile information situation. It limits inquiry inactivity by advanced the most high-performing suppliers. Scalia beneficially considers repositioning of just picked fights that may by and large cut down the limit cost. The facilitated administration can be worked by an autonomous intermediary for different clients.
They described [12] a practical two-cloud Oblivious RAM protocol that reduces the client-server bandwidth cost to about 2:6 times that of simply reading or writing the block from non-oblivious cloud storage. They proposed a novel commutative checksum-encryption construction that allows our multi-cloud ORAM protocol to efficiently protect the privacy of the access pattern against one malicious cloud. They provide a full-edged implementation of our 2-cloud ORAM system, and report results from a real-world deployment over Amazon EC2 and Microsoft Azure. In practice, each cloud can distribute the data across multiple servers. For simplicity, they will first regard each cloud as a single logical entity; then in the full online version.

The use of multiple cloud [16] providers for gaining security and privacy benefits is nontrivial. They propose a set of four distinct multicloud architectures. Given that each kind of multicloud approach can be categorized as one of these four classes, this infers a cutting edge that is to some degree disappointing. An aggressor that approaches the distributed storage segment can take depictions or adjust information in the capacity. This triggered a lot of research activities, resulting in a quantity of proposals targeting the various cloud security threats. Close by with these security issues, the cloud worldview accompanies another arrangement of one of a kind highlights, which open the way toward novel security methodologies, procedures, and structures.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

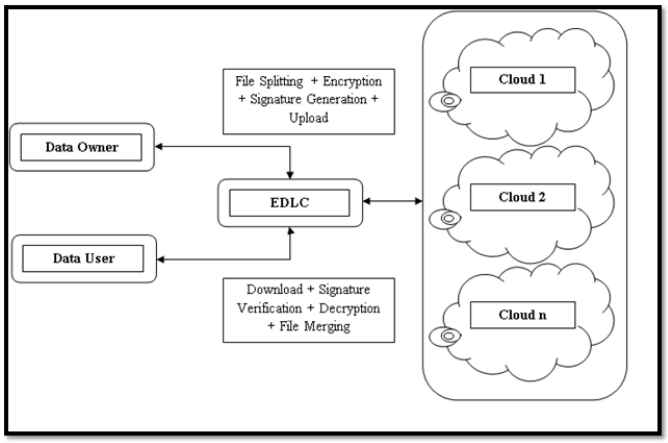
DOI 10.17148/IJARCCE.2021.10328

IV. SECURITY IN CLOUD COMPUTING

In order to keep the Cloud secures [13], these security threats need to be controlled In addition information dwelling in the cloud is additionally inclined to various dangers and different issues like classification and honesty of information ought to be considered while purchasing stockpiling administrations from a cloud specialist organization. In this paper different security worries for Cloud processing condition from numerous point of view and the answers for anticipate them have been exhibited analysed and ordered. This broad overview paper expects to expand and dissect the various uncertain issues debilitating the Cloud figuring appropriation and dissemination influencing the different partners connected to it. Utilizations dynamic groups conspire, whereby predicates are analysed over encoded information and multiparty registering.

Every calculation [14] is gone for unravelling a specific hazard. Anyway distributed computing is as yet battling in its earliest stages, with positive and negative remarks made on its conceivable usage for a vast estimated venture. Its security insufficiencies and advantages should be painstakingly weighed before settling on a choice to actualize it. However along with these advantages, storing a large amount of data including critical information on the cloud motivates highly skilled hackers thus creating a requirement for the security to be considered as one of the best issues while considering Cloud Computing. The cloud is just usable through the Internet so Internet dependability and accessibility is basic.

V. ARCHITECTURE OF THE PROPOSED SYSTEM



I.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.

II.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.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 10, Issue 3, March 2021
DOI 10.17148/IJARCCE.2021.10328

III.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.

VI. ALGORITHM

Algorithm 1: File Splitting and Encryption

- **Input:** Text file, secret key
- **Output:** Encrypted Files E (F.1), E (F.2), E (F.3), E (F.4), and E (F.5)
- **Step 1**: Uploads a file (F) and give user defined secret key (SK)
- **Step 2**: Find the size of a file (SF)
- **Step 3**: Slice or Divide the size of a file (SF) by the service providers integrated with Multi Cloud.
- **Step 4**: Index based files (F.0, F.1, F.2, F.3 and F.4) are created with the same file name and get stored in the owner's local machine.
- **Step 5**: Pass the user defined secret key (SK) to the Unicode Encoding Object to initialize a key(K) and Vector (IV) which can be used to protect repetition pattern in encrypted files.
- **Step 6**: Encrypt each part of the sliced file E (F.1), E (F.2), E (F.3), E (F.4), and E (F.5) from local server and store in the Multi Cloud server.
- **Step 7**: End

Algorithm 2: File Decryption and Merging

- Input: File Name, Secret key (SK)
- Output: Decrypted File parts and Merged to get File (F)
- Step 1: Get the File Name (FN) and Secret Key (SK) from the data owner or File owner by making request to the processor
- Step 2: Enter or Pass that File Name (FN) and secret Key (SK)
- Step 3: 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).

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10328

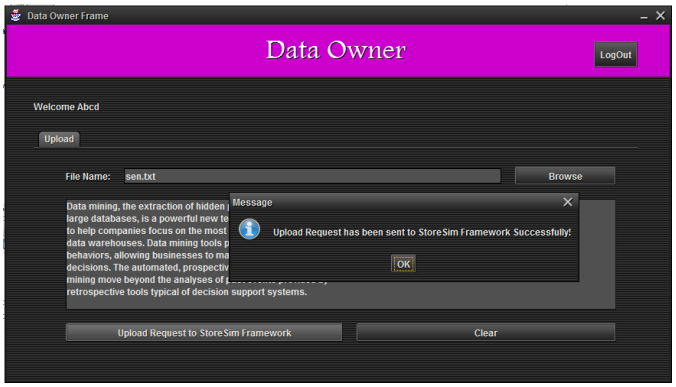
- Step 4: Pass the user defined secret key (SK) to the Unicode Encoding Object to initialize a key (K) and a vector (V) which can be used to create symmetric Decrypt or object.

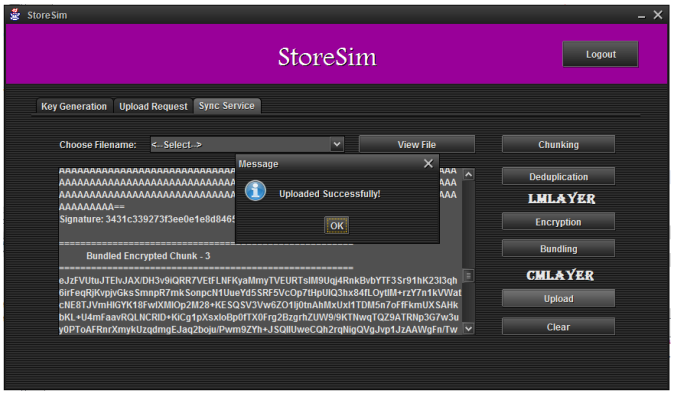
- Step 5: Merge each part of the decrypted files F1, F2, F3, F4, and F5 from Multi Cloud storage service provider to obtain the original file F.

- Step 6: Auto removal of all decrypted and encrypted parts of the files stored in the respective services.

- Step 7: End

VII. RESULTS





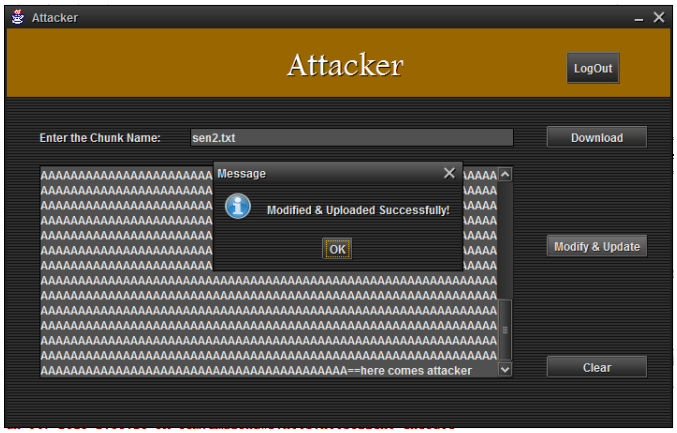
IJARCCE

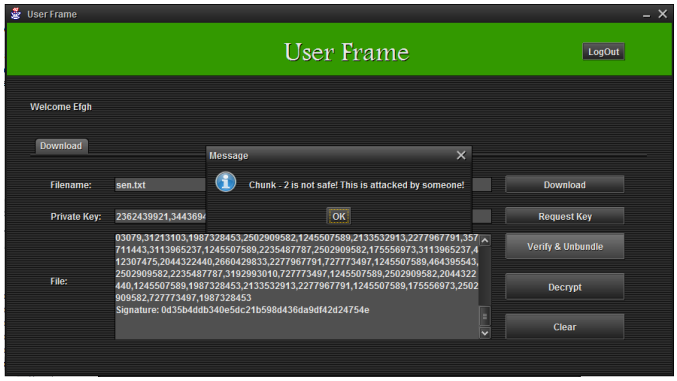
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10328





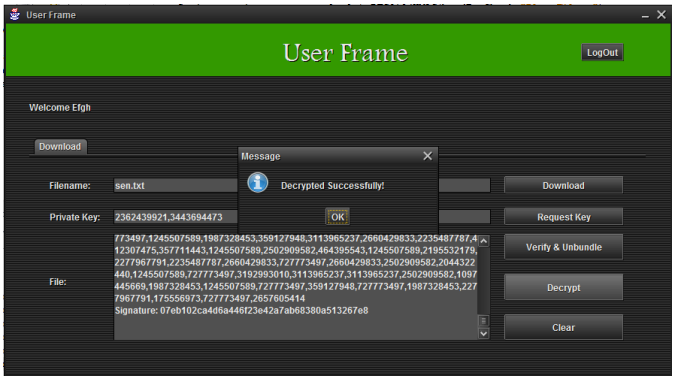
IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 3, March 2021

DOI 10.17148/IJARCCE.2021.10328



VIII. CONCLUSION AND FUTURE WORK

On this paper, 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. Previous paper has focused on measurement analysis of cloud storage services only. 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. The receiver sends the decryption request to the owner or the owner can share the required credentials through Bring Your Own Secure Channel (BYOC) or out of band procedure.

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.