Encryption Technique to Optimize Information Leakage in Multi Cloud Storage Services

M.Vijaya Madhuri, M.V.Sangameswa

ABSTRACT--- Multicloud is one such aspect which is considered as the vision of the future. It includes distribution of data for the user automatically by means of cloud storage providers (CSPs) which in turn provides a considerable degree of control over information leakage. Due to the process of unplanned distribution of data chunks will result in disposing the crucial information while using multiple clouds. A storage system named Storesim is introduced in Multicloud to store syntactically relevant data on the assigned cloud, thereby limiting the intensity of leakage of information across those clouds. During this survey it has been identified that few CSP's of some Multicloud services got compromised under coercion. In this paper, we made use of the Ultramodern Encryption Standard (UES) into storesim thereby avoiding unauthorized access to the information present in the Multicloud ensuring better level of security to CSP's implicating reduced information leakage.

INTRODUCTION

With the inexorably fast take-up of gadgets, for example, PCs, cell phones and tablets, clients require a universal and gigantic system stockpiling to deal with their consistently developing computerized lives. To fulfil these needs, many cloud-based capacity and record sharing administrations, for example, Dropbox, Google Drive and Amazon S3, have picked up notoriety due to the simple to-utilize interface and low stockpiling expense. In any case, these brought together distributed storage administrations are censured for getting the control of clients' information, which enables stockpiling suppliers to run investigation for showcasing and promoting. Likewise, the data in clients' information can be spilled e.g., by methods for malevolent insiders, secondary passages, influence and compulsion. One conceivable answer for lessen the danger of data spillage is to utilize Multicloud capacity frameworks in which no single purpose of assault can release all the data. A noxious element, for example, the one uncovered in late assaults on protection, would be required to force all the diverse CSPs on which a client may put her information, so as to get a total image of her information. Put essentially, as the maxim goes, don't place all the investments tied up on one place.

However, the circumstance isn't so straightforward. CSPs, for example, Dropbox, among numerous others, utilize resync-like conventions [7] to synchronize the nearby record to remote document in their incorporated mists [8]. Each nearby document is parcelled into little lumps and these pieces are hashed with fingerprinting calculations, for example, SHA-1, MD5. Therefore, a record's substance can be remarkably recognized by this rundown of hashes. For each update of nearby record, just lumps with changed hashes will be transferred to the cloud. This synchronization dependent on hashes is not quite the same as diff - like conventions that depend on contrasting two forms of a similar document line by line and can distinguish the accurate updates and just transfer these updates in a fix style.

2. LITERATURE REVIEW:

In this area, we did a survey a portion of the writing identified with the four unmistakable mainstays of our work, which are as per the following:

Untrusted storage cloud: Depot [11] and SPORC [12] expected that the capacity mists are untrusted and deficiency inclined secret elements. Nonetheless, both their work utilized just a solitary cloud which has both figure and capacity limit. Our work is distinctive since we consider a Mutlicloud in which every capacity cloud is just filled in as capacity without the capacity to process. The prior past work, for example, Cooperative File System (CFS) [13] and Samsara [14] structured their capacity framework with a shared system contained conceivably untrusted hubs. Our work focuses to utilize capacity cloud without utilizing decentralized P2P proto-col [15] and upgrades information arrangement in a unified manner. This paper expands our work on StoreSim [16].

Multicloud storage services Our work isn't the only one in putting away information with the appropriation of various CSPs, e.g., SPANStore [5], DepSky [2] and NCCloud [3]. However, these work concentrated on various issues, for example, cost optimization [5], information consistency and accessibility [2] and administration reaction time [17]. Different endeavours [18] on the cloud orchestration gave organization designs as far as the trade-off among cost and execution. In contrast to these works, our work centres around the data spillage improvement for capacity administration in a Multicloud domain by abusing data similitude brought about by the synchronization of changed information. Beneficial endeavours on defeating vendor lock-in, DepSky [2] limited the expense of information move starting with one cloud then onto the next by putting away just a small amount of the aggregate sum of information in each cloud while Scalia [4] utilized the

Revised Manuscript Received on August 14, 2019.

M.Vijaya Madhuri, CSE ,Faculty of Engineering, Godavari Institute of Engineering and Technology (A) Rajahmundry ,AP,India. (E-mail: mynameischakry@gmail.com)

Dr.M.V.Sangameswar, Professor CSE ,Faculty of Engineering, Godavari Institute of Engineering and Technology (A) Rajahmundry ,AP,India.

information replication at a higher stockpiling cost. Be that as it may, in StoreSim, we give a client explicit load to each cloud which not just organizes the portion of capacity load for each cloud yet additionally avoids the data spillage over the CSPs. Different examinations have concentrated on estimation analyysis of distributed storage administrations [8], [9]. Their work gave us numerous experiences on planning StoreSim. Be that as it may, their work neglected to uncover improvement parts of data spillages of the business CSPs they contemplated.

Cloud security. Numerous examinations [19], [20], [21] centre around security and protection perspectives which are real obstructions of cloud reception for the two people and organizations. Previous work [20] proposed a semantic system dependent on publicly supporting to decide the affectability of things and differing frames of mind of clients towards security. Bohli et al. [19] gave a study to four diverse multicloud architectures with different security and protection improving plans. The engineering of StoreSim is one of them, which permits appropriating fine-grained sections of the information to unmistakable mists. Our work further executes the StoreSim framework with new data spillage measures.

Near Duplicate Deteciton: Li et al. [22] proposed a Privacy misfortune measure dependent on the JS-disparity separation which is a technique for estimating the comparability between two likelihood disseminations. Motivated by their work, we plan our data spillage capacity dependent on closeness. To figure the data spillage, we have to process the pairwise likenesses. MinHash [23], [24] and SimHash [23], [25] were intended for identifying the close copy site pages dependent on Jaccard and Hamming separation, separately. Notwithstanding, their work can't have any significant bearing to our work legitimately because of substantial calculation and high stockpiling overhead. As far as we could possibly know, this is the main work which applies close copy methods for counteracting data spill age in multicloud stockpiling administrations.

3 ARCHITECTURE-STORESIM:

The engineering of StoreSim is appeared in Figure 1. It very well may be seen that there is a trust limit between the metadata and capacity servers. We expect that customers and metadata servers, which are arranged inside the trust limit, are trustable by clients while remote servers outside the limit are deceitful. For instance, the metadata can be put away in private database servers while capacity servers can be found open CSPs, for example, Amazon S3, Dropbox and Google Drive. Capacity servers can be gotten to through standard APIs (Application Programming Interfaces). As it appeared in Figure 1, all control streams are inside the trust limit while information streams can cross the trust limit. So as to enhance the data spillage, we structure two parts in StoreSim. The main segment is the Leakage Measure layer (LMLayer) that is utilized to assess the data spillage and further to create the capacity plan which maps information pieces to various mists. The other part is the Cloud Manager layer (CMLayer) that gives cloud interoperability in a syntactic way. In the accompanying, we will initially introduce how we model metadata and capacity cloud. we present BFSMinHash, a Bloom filter sketch for MinHash in order to reduce storage overhead.

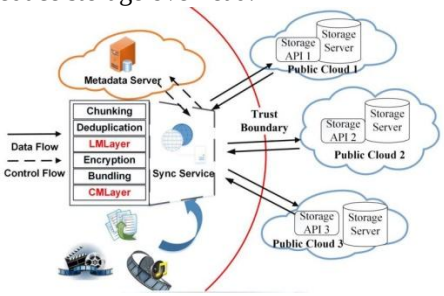

Figure 3.1 : Architecture of Storesim

4. PROPOSED SYSTEM:

In order to provide storage services at an affordable low cost , the vast cumulative of personal data of the user which can be further monitored by Dropbox and Google Drive, are centralized repositories considered as cloud storage services. There is a scope that the users may lose their control over the data while utilising the storage services. Recent news about PRISM[26] states that the CSP's got compromised under coercion. To avoid that situation which in turn provides better control over the data we use Ultramodern Encryption Standard(UES)[27] technique that enhances the control over the user data .

5. ULTRAMODERN ENCRYPTION STANDARD ALGORITHM(UES):

Ultramodern Encryption Standard (UES) for secure data transmission which uses prolic series number for generating set of keys, binary and gray code operations for encryption and decryption processes. If an intruder intercepts the message, it is difficult to decipher the message because of multilevel cipher rounds used in this algorithm[27].

5.1 Key generation process The key generation of UES

Algorithm starts by selecting an arbitrary prolic series number following the relation Tn= n*(n+1) such that $0 \leq n \leq 255$, the ASCII character range, it is being represented as 17 bit binary code. The binary code is converted to 17 bit gray code i.e., 34 bits were considered, the process continues till it generates 272 bit key. Now the generated 272 bits are divided into 34 blocks of 8 bits each, which are being used as set of keys for encryption and decryption process.

5.2 Encryption process

The process of encoding a message m with proper key(s)k and encryption algorithm E in such a way that only authorized users can access it is termed to be as encryption, which generally represented as cipher text c= ***E***(k,m)[28]. The encryption process starts with giving 8 bit plaintext as an input, there after it undergoes 16 rounds of encryption where 32 blocks of key 8 bits each are being used. Finally the process would halt by operating two output transformations using 2 blocks of key 8 bits each. Detailed execution of encryption and one round of encryption are illustrated in the Fig2 and Fig3 respectively

Figure 5.2 Encryption of UES

Where ICTR# indicates Intermediate Cipher text of the corresponding Round.

Output T# indicates Output Transformation,

ICTOT# indicates Intermediate Cipher text of the Output Transformation.

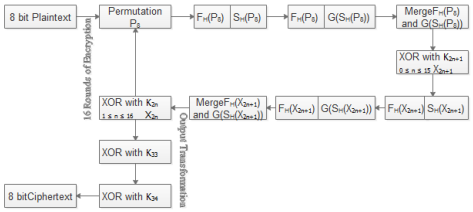

Figure 5.3 Detailed Execution of one round of Encryption in UES

Where FH: First Half
SH: Second Half
G: Gray code

6. RESULTS:

Ultramodern Encryption Standard which primarily focus on handling sensitive data and providing security to the data which provides a better level of control over the data thereby assuring reduced leakage in the multicloud. The following screenshots describes the results in detail .

Figure 6.1 Home page

Figure 6.2 Client Registration

Figure 6.3 Client Login

Figure 6.4 Client Home

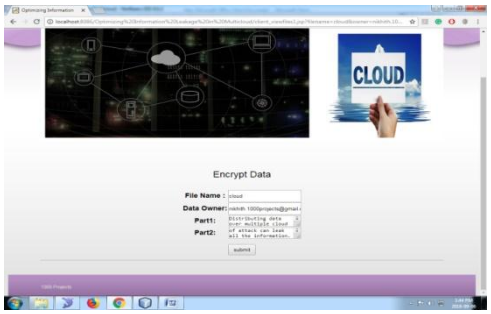

Figure 6.5 Upload File

Figure 6.6 Encrypt Data

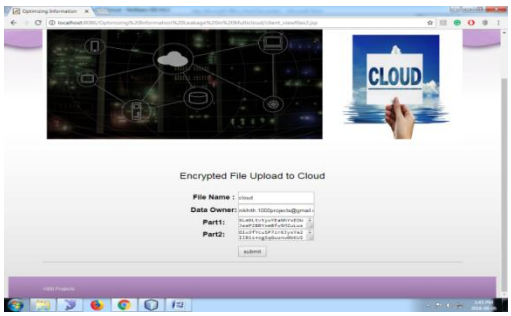

Figure 6.7 File Upload to Cloud

7. CONCLUSIONS:

The presence of coercion which was identified in few CSP's has been limited by the usage of UES algorithm and better level of security has been observed. Thereby the level of leakage in the Multicloud has been further optimized.

REFERENCES:

1. J. Crowcroft, "On the duality of resilience and privacy," in Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 471, no. 2175. The Royal Society, 2015, p. 20140862.
2. A. Bessani, M. Correia, B. Quaresma, F. Andre,´ and P. Sousa, "Depsky: dependable and secure storage in a cloud-of-clouds," ACM Transactions on Storage (TOS), vol. 9, no. 4, p. 12, 2013.
3. H. Chen, Y. Hu, P. Lee, and Y. Tang, "Nccloud: A network-coding-based storage system in a cloud-of-clouds," 2013.
4. T. G. Papaioannou, N. Bonvin, and K. Aberer, "Scalia: an adaptive scheme for efficient multi-cloud storage," in Proceedings of the International Conference on High Performance Computing, Networking, Storage and Analysis. IEEE Computer Society Press, 2012, p. 20.
5. Z. Wu, M. Butkiewicz, D. Perkins, E. Katz-Bassett, and H. V. Madhyastha,"Spanstore: Cost-effective geo-replicated storage spanning multiple cloud services," in Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles. ACM, 2013, pp. 292–308.
6. G. Greenwald and E. MacAskill, "Nsa prism program taps in to user data of apple, google and others," The Guardian, vol. 7, no. 6, pp. 1–43, 2013.
7. T. Suel and N. Memon, "Algorithms for delta compression and remote file synchronization," 2002.
8. I. Drago, E. Bocchi, M. Mellia, H. Slatman, and A. Pras, "Benchmarking personal cloud storage," in Proceedings of the 2013 conference on Internet measurement conference. ACM, 2013, pp. 205–212.
9. I. Drago, M. Mellia, M. M Munafo, A. Sperotto, R. Sadre, and A. Pras, "Inside dropbox: understanding personal cloud storage services," in Proceedings of the 2012 ACM conference on Internet measurement conference. ACM, 2012, pp. 481–494.
10. U. Manber et al., "Finding similar files in a large file system." in Usenix Winter, vol. 94, 1994, pp. 1–10.
11. P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish, "Depot: Cloud storage with minimal trust," ACM Transactions on Computer Systems (TOCS), vol. 29, no. 4, p. 12, 2011.
12. A. J. Feldman, W. P. Zeller, M. J. Freedman, and E. W. Felten, "Sporc: Group collaboration using untrusted cloud resources." in OSDI, vol. 10, 2010, pp. 337–350.
13. F. Dabek, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica, "Wide-area cooperative storage with cfs," in ACM SIGOPS Operating Systems Review, vol. 35, no. 5. ACM, 2001, pp. 202–215.
14. L. P. Cox and B. D. Noble, "Samsara: Honor among thieves in peer-to-peer storage," ACM SIGOPS Operating Systems Review, vol. 37, no. 5, pp. 120–132, 2003.
15. H. Zhuang, R. Rahman, and K. Aberer, "Decentralizing the cloud: How can small data centers cooperate?" in Peer-to-Peer Computing (P2P), 14-th IEEE International Conference on. Ieee, 2014, pp. 1–10.
16. H. Zhuang, R. Rahman, P. Hui, and K. Aberer, "Storesim: Optimizing information leakage in multicloud storage services," in Cloud Computing Technology and Science (CloudCom), 2015 IEEE 7th International Conference on. IEEE, 2015, pp. 379–386.
17. S. Choy, B. Wong, G. Simon, and C. Rosenberg, "A hybrid edge-cloud architecture for reducing on-demand gaming latency," Multimedia Systems, pp. 1–17, 2014.
18. T. Zou, R. Le Bras, M. V. Salles, A. Demers, and J. Gehrke, "Cloudia: a de-ployment advisor for public clouds," in Proceedings of the VLDB Endowment, vol. 6, no. 2. VLDB Endowment, 2012, pp. 121–132.
19. J.-M. Bohli, N. Gruschka, M. Jensen, L. L. Iacono, and N. Marnau, "Security and privacy-enhancing multicloud architectures," Dependable and Secure Computing, IEEE Transactions on, vol. 10, no. 4, pp. 212–224, 2013.
20. H. Harkous, R. Rahman, and K. Aberer, "C3p: Context-aware crowdsourced cloud privacy," in 14th Privacy Enhancing Technologies Symposium (PETS 2014), 2014.
21. I. Ion, N. Sachdeva, P. Kumaraguru, and S. Capkun, "Home is safer than thecloud!: privacy concerns for consumer cloud storage," in Proceedings of the Seventh Symposium on Usable Privacy and Security. ACM, 2011, p. 13.
22. T. Li and N. Li, "On the tradeoff between privacy and utility in data publishing," in Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM, 2009, pp. 517–526.
23. [23]M. Henzinger, "Finding near-duplicate web pages: a large-scale evaluation of algorithms," in Proceedings of the 29th annual international ACM SIGIR conference on Research and development in information retrieval. ACM, 2006, pp. 284–291.
24. P. Li and C. Konig,¨ "b-bit minwise hashing," in Proceedings of the 19th international conference on World wide web. ACM, 2010, pp. 671–680.
25. G. S. Manku, A. Jain, and A. Das Sarma, "Detecting near-duplicates for web crawling," in Proceedings of the 16th international conference on World Wide Web. ACM, 2007, pp. 141–150.
26. G. Greenwald and E. MacAskill, "Nsa prism program taps in to user data of apple, google and others, " The Guardian, vol. 7, no. 6, pp 1–43, 2013.
27. P.Sri Ram Chandra , G.Venkateswara Rao , G.V.Swamy "Ultramodern Encryption Standard Cryptosystem using Prolic Series for Secure Data Transmission" International Journal of Latest Engineering Research and Applications (IJLERA) ISSN: 2455-7137 Volume – 02, Issue – 11, November – 2017, PP – 29-35
28. Delfs, Hans &Knebl, Helmut (2007). "Symmetric-key encryption". Introduction to cryptography: principles and applications. Springer. ISBN 9783540492436.