Distributed cloud Storage Image Control Reliability and Obliging Provable Data and Confirmation

Eshwari Devi Jagapur [1]

[1] *Assistant Professor, Department of CSE, Canara Engineering College, Benjana Padavu, Mangaluru, Karnataka*

***Abstract*— Data integrity is very important while storing few data in multi-cloud. Distributed cloud storage is the method of storing the data in obliging provable data for the reliability confirmation. this paper proposes the integrity of data while storing distribute cloud this technique improve can improves overall enterprise performance by avoiding vender lock-in for customers to minimize the computation cost this technique also reduces cost while computation is reflected in performance analysis.**

***Index Term*- Storage security, provable data possession, Visual Cryptography, Steganography, multiple cloud, cooperative.**

I. INTRODUCTION

The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer called Cloud Computing. Sharing of computing resources (hardware and software) solves very complex problems [1] and distributed cloud problems of any kind typically the network problems. Cloud computing has the capability to incorporate multiple internal and/or external cloud services together to provide [11] high interoperability. Called distributed cloud as a multi Cloud environment.

Distributed cloud storage is the method of storing files in the distributed manner. Any cloud service provider cannot guarantee the security of inherent attacks from outside of enterprise cloud in cases[12] data leakage and tag forgery attack. possible the file systems shares some similar features like files are split into blocks or chunks and stored on block servers and distributed cloud storage platform used for managing client data. However, if such an important platform is vulnerable to the attacker, it would bring irretrievable and losses to the clients. For example, the confidential data can be illegally accessed through a remotely provided by a multi-cloud, or from which relevant data and archives will be lost or tampered when they are stored into an uncertain storage areas. Hence this paper provides few security technique to manage few storage services and providing few data integrity while storing any kind of files or data.

II. ORGANIZATION OF PAPER

Security is the main issue in cloud computing where [2] Banerjee (2009) provides an overview of cloud scale intelligent infrastructure attacks. The challenges like user interface, task distribution and coordination issues are addressed and evaluated by [3] (Lijun, chan,& TSE,2008).Grossman et al.(2009) developed a cloud-based infrastructure which had been optimized for wide area performance networks and supported necessary data mining application [4] Praveen &Betsy(2009) provided a comprehensive introduction to the application of cloud in universities. As various security models have been proposed for existing methods model cannot cover all security requirements for example privacy preservation and ownership authentication for these kind of problems I have constructed obliging [10] provable data for the distributed cloud storage.
[5]Grossman et a1, (2009) developed a cloud-based infrastructure which had been optimized for wide area, performance networks and supported necessary data mining applications. Cloud computing infrastructures accelerated the adoption of different technological innovations in academia and its facilities and resources could be accessed by the colleges as on–demand. [6]Delic & Riley (2009) assessed the current state of the Enterprise Knowledge Management and how it would turn into a more global, dependable and efficient infrastructure namely cloud computing. They discussed architectural technologies and related applications. The basic features of cloud computing are presented and compared with the original “Grid Computing” technology (Aymerich, Fenu & Surcis, 2008).

Distributed Cloud provides the opportunity of flexibility and adaptability to use the computing resources on-demand. Contrary to having only one service provider, different providers use different interfaces to their compute resources utilizing varied architectures and implementation technologies for customers. Although this creates a management problem, a common architecture facilitates the management of compute resources from different Cloud providers in a homogenous manner [9](Dodda, Smith & van Moorsel, 2009). Mitchell (2008) provided an overview of existing learning architectures, and raised questions about how educational institutions are managing the cloud computing resources. He also brought reasonable explanations for the challenge of indexing web resources for optimum discoverability by students and educators.

After brief summary/literature Review infrastructure, application and service aspects of cloud computing and how it will support for secure manner.

III. METHODOLOGIES: DATA INTEGRITY BY OPDP ALGORITHM

Architecture as shown in Figure 1 consists of trusted client as well as three or more cloud service providers that provide Database as a Service. The Database as a Service providers provides reliable content storage and data management, but are not trusted by the clients to preserve content privacy Authority. The client does not store any persistent data but stores a mapping table describing the storage of various fragments location, their names etc. However the client has access processing power. temporary storage & functionality in terms of offering a DBMS frontend, reformulating, & optimizing queries & post processing query results, all of which are fairly cheap and can be performed using inexpensive hardware. The client executes queries by transmitting appropriate sub queries to each database and then piecing together the result obtained from the Cloud service providers at the client side.

A. TPA:

An existing user has to upload the file using As Encryption usually takes longer time to break the key. Where the verification and transaction will be done through uploading file. The uploaded file will be splitted by Tpa into different blocks to be stored on three different servers.

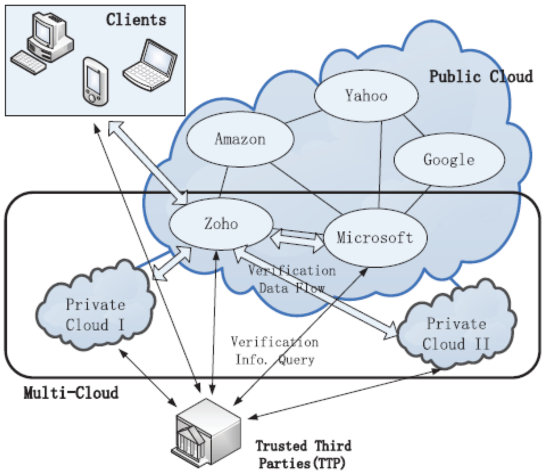

Figure 1: Multi-cloud Architecture

Security key passed between user and the TPA: The key would be generate on a random function with 10000 possible numbers as argument increasing the permutation of numbers tenfold. This key act as a file block identification and as secured password for decryption.

File Alerts to the third party auditor: If and when any modification done by the cloud service provider leads to sending of file modification alerts to the TPA by the system with block number and server number thus triangulating the cause of modification.

B. Data Storage:

Consider the data is stored at a single [8] Cloud storage as a Service provider. Then there is a single point of failure which will affect data availability. [7] Availability is also one of the issue if runs out of business. Cloud service customers cannot rely on single Cloud service provider to ensure storage of vital data. If the database is stored at two storage providers, there are chances that the two CSPs achieve a fraudulent can exchange the part of the data with each other & reconstruct the whole data. In our approach, the client does not have to trust the administrators of any cloud service providers to guarantee privacy. As long as an adversary does not gain access to all the data, data privacy is fully protected. If the client were to obtain database services from different vendors, the chances of an adversary breaking into all the service providers, is greatly reduced.

C. Verification

Once the file has been approved by cloud, it can be viewed and downloaded by end user**.**

The following are the design requirements the cloud user will divide the file into 'N' number of blocks and has to be uploaded to the specified cloud server (Cs1, Cs2 & Cs3).

1. The Cloud server has to authorize the valid remote users. If the Remote user is an attacker then attacker has to blocked to the cloud server. The data should be integrated by the cloud server.
2. The Third party auditor has to maintain the error localization and has to monitor the Cloud Server Activities.

Technique:

There are two basic ways to [15]hide digital signature of the image in shares of the participants, which can be used for cheat-detection of the shares in case it is suspected that a cheater has produced a fake share. The first approach hides the same digital signature in all shares and it requires the original digital signature for verification. The second approach hides the bits of digital signature in different shares at random locations by using a key K. In case of suspicion, the signature can be extracted in presence of all shares and compared with the signature generated from the reconstructed image. [14] We focus in this paper on the second approach, because it does not require the original signature for cheat-detection.

The algorithm for hiding signature or data in the proposed method is given below:

For each character do:

- Convert every character in digital signature into binary "0" and "1",
- Select a random share si,
- Find a random block from the share si by using seed value as a key K,

- Check whether binary value of signature is “0” or “1”,
- Check whether the block in the share si is either white or black share,
- If signature bit is “1” and the block is white,
- Find a random black subpixel from the block, and flip it,
- If signature bit is “1” and the block is black,
- Find a random white subpixel from the block, and flip it.

Selection of a share for hiding a binary “1” is done by tossing, because bits can be hidden in any one of the shares. No change is done for hiding “0” and corresponding and identical white blocks are considered to contain “0”. But change is done for hiding binary “1” by flipping a white (black) subpixel in one of the blocks of black (white) share. Flipping a white subpixel in a black share ensures that the black share is still recovered as black on stacking qualified shares. Similarly, flipping a black subpixel in a white share makes the white share recoverable as white.

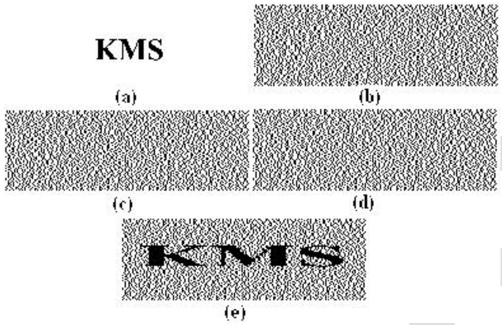

Fig.3 Example of Image: (a) Original image, (b) Cloud 1, (c)Cloud 2 and (d) Cloud 3 and (e) Decrypted image.

IV. IMPLEMENTATION & PERFORMANCE ANALYSIS

We established [12] cloud in our laboratory which provides infrastructure as services. Used IBM system x3500 M4 server as a high end server and vSphere Exsi 5.5 as a hypervisor. VSphere client. Makes tpa as well as cloud service provider uses server IP address as static because when IP address is made as one the same IP address will remain for all time and we can easily use the same IP address though the network. If IP address is dynamic then it always changes, each time when we boot the system we need to configure client again. Change [16] DNS server address as well as gateway address if wants to connect external network. Internet provider DNS address as well as gate way address should be added if we want to connect the server to internet.

A. Data integrity Algorithm

```
1.  Input file F
2.  Splitfilen-blocks,indexing,          {β1, β2, β3}
3.  .Generate key  for each block
4.  .KeyGen (β)   ⟹   {sk, pk}
     Compute, β = β1, β2   ⟸   $\{0,1\}^k$
     ¥ = (α, β)
     Where, ¥=α*β, product of two primes.
5.  Generate Tag  for each block
6.  Tag Block(sk, pk, mi, vi, i) → {Ti, hi}
     Compute, T*i = gmi mod N
     H*i= Hk1 (Ti || f (vi) || i)
     Where, H=cryptographic hash function
     f = pseudo random function

7.  Store all the credentials in the form of tags and hash
    on the TTP before uploading the data on clouds.
```

Notation	Representation
A	No of block in file
B	No of sector in each block
T	number of index coefficient pairs in a query
C	number of clouds to store a file
F	file with n*s sectors; F= {mi,j}, i Є [1,n], j Є [1,s]
σ	set of tags; σ = {σi}, i Є [1,n]
H	Set of hash values; H = {hi}, i Є [1,n]
V	set of number of times ith block is modified; i Є [1,n]

Table No 1: Notations of data integrity

The performance of proposed system is better than normal cloud. As we observed in the performance of the system, we can see the reduction of block usage as well as file usage taking place. Virtual networking concept is used. Same way the memory usage is proper and a normal user didn’t faced any extra problem. The normal user’s services not get slowdown in cloud environment.

As the size increases the time increases interms of the kb file size. It can be shown interms of probability of time to upload the file by n number of users as formulated below

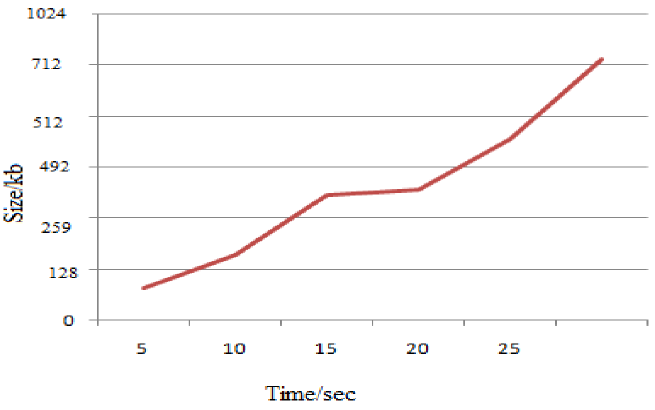

Figure 2: Performance of server

Performance of cloud can be measured .as the file size increases the time also increases. The above value takes all the experimental values from different readings with respect to network.

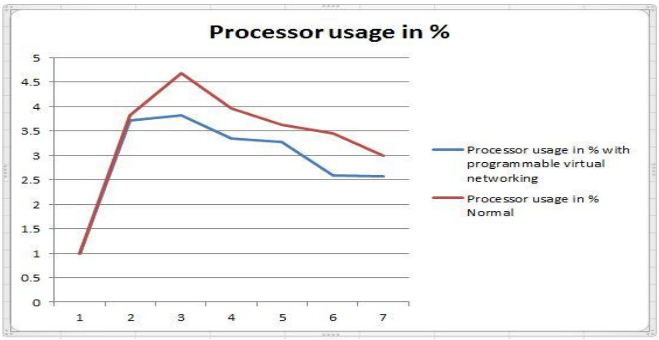

Figure 3: processor usage

The performance of the system is better compared to the existing one. As we observed in the performance of the system, we can see the reduction of resource usage taking place. The processor usage is reduced a little when programmable virtual networking concept is used. Same way the network usage is proper and a normal user didn't faced any extra traffic while attack detection process was going on. The normal users services not get slowdown in this case.

VI. CONCLUSION

A new secured, cost effective, highly available multi-cloud architecture for enabling privacy-preserving outsourced storage of data has been introduced. The solution seeks to provide each customer with a better cloud data storage decision, taking into consideration the user budget as well as providing him with the best quality of service (security, response time and availability of data) offered by available cloud service providers. Fragmentation of data into chunks which preserve privacy are used to decompose data which makes the data invaluable even if an intruder gets access to this data in this multi-cloud architecture Using multiple data providers that have much high failure probability than the leading provider is sufficient to guarantee high availability Storage providers. By addressing the requirements, a storage vendor or cloud provider will be able to create a multi-tenant storage infrastructure that is secure, flexible, highly functional and interoperable.

REFERENCES

[1]. Basappa B. Kodada, Gaurav Prasad, Alwyn R. Pais, *"Protection against DDoS and Data Modification Attack in Computational Grid Cluster Environment*", MECS Publisher – IJCNIS 2012, ISSN: 2074-9090 (Print), ISSN: 2074-9104 (Online), Vol. 4, No. 7, July 2012

[2]. Banerjee *(*2009*)* provides an overview of technological researches performed in HP labs, and a cloud-scale intelligent infrastructure attracts.

[3]. Grossman et *a1*, *(*2009*)* developed *a* cloud-based infrastructure which had been optimized *for* wide area,performance networks *and* supported necessary data mining

[4]. Praveena& Betsy, (*2009*) *provided a comprehensive introduction* to *Praveena*, K., *& Betsy* T.(*2009*).*www.academia.edu/.../877-0428_Effective_use_of_cloud_computing*

[5]. Grossman et a1, *(*2009*)* developed *a* cloud-based infrastructure which had been optimized *for* wide area, performance networks *and* supported necessary data mining.www.academia.edu/.../877-0428_Effective_use_of_cloud_computing_in

[6]. Delic *&* Riley *(*2009*)* assessed the current state of the Enterprise Knowledge would turn into *a* more global, dependable *and* efficient infrastructure namely cloudwww.academia.edu/.../877-0428_Effective_use_of_cloud_computing_in...

[7]. K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in ACM Conference on Computer and Communications Security, E. AlShaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 187–198

[8]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep.,

[9]. Y. Dodis, S. P. Vadhan, and D. Wichs, "Proofs of retrievability via hardness amplification," in TCC, ser. Lecture Notes in Computer Science, O. Reingold, Ed., vol. 5444. Springer, 2009, pp. 109–127.

[10]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, SecureComm, 2008, pp. 1–10.

[11]. H. Shacham and B. Waters, "Compact proofs of retrievability," in ASIACRYPT, ser.Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90

[12]. G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. N. J. Peterson, and D. X. Song, "Provable data possession at untrusted stores," in ACM Conference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598–609

[13]. A. Juels and B. S. K. Jr., "Pors: proofs of retrievability for large files," in ACMConference on Computer and Communications Security, P. Ning, S. D. C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 584–597.

[14]. D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology (CRYPTO'2001), vol. 2139 of LNCS, 2001, pp. 213–229

[15]. O. Goldreich, Foundations of Cryptography: Basic Tools. Cambridge University

[16]. L. Fortnow, J. Rompel, and M. Sipser, "On the power of multiprover interactive protocols," in Theoretical Computer Science, 1988, pp. 156–161.

AUTHORS PROFILE

. Ms.Eshwari Devi Jagapur received his B.E degree in computer science and engineering from Sri Taralabal Jagadgur Institute of Technology, Ranebennur in 2012. Currently working as Asst.professor Dept of Computer science and engineering at Canara Engineering College Mangalore. Her area of interest is Computer Networks, Cloud Computing and Oracle.