Joint Collaboration Structure For Multi Cloud Frameworks And Security Issues

B.Mahesh, D.Durgaprasad

(B.Mahesh) Computer Science And Engineering, Baba Institute Of Technology And Sciences,Visakhapatnam, India;
(D.Durga Prasad) Computer Science And Engineering, Baba Institute Of Technology And Sciences,Visakhapatnam, India.
Email: b.mahesh498@gmail.com

ABSTRACT: Cloud computing has emerged as a popular paradigm that offers computing resources (e.g. CPU, storage, bandwidth, software) as scalable and on-demand services over the Internet. The multi-cloud environment can end the vendor lock-in of the consumer which is a trait in the single cloud. The significant zone of concern in this field is the understanding between the cloud service providers for collaboration of their services in multi-cloud. Data fragmentation plays an important role in data distribution. In this paper, we proposed a mixed fragmentation technique for data distribution through the collaboration multi-cloud model which holds an economical distribution of data among the available Service Providers in the market, to provide customers with achievable distributing merits which intern includes preserving confidentiality, integrity and availability(CIA) perimeters by making use of multiple distinct clouds simultaneously.

Keywords : Internet, Cloud computing, Framework, Cloud services, Multi-tenant, Security.

1 INTRODUCTION

The end of this decade is marked by a paradigm shift of the industrial information technology towards a subscription based or pay-per-use service business model known as cloud computing. Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management. Cloud data storage, in which, subscribers do not have to store their own data on their servers, where instead their data will be stored on the cloud service provider's servers. In Cloud data storage we observed that, from a customer's point of view, relying upon a single SP for his outsourced data is not very promising. In addition, providing CIA perimeters can be achieved by dividing the user's data block into data pieces and distributing them among the available SP's.

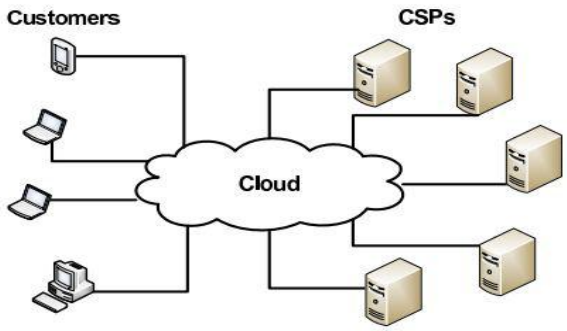

Fig1: *Cloud computing Architecture example*

The scenario of multi-cloud presents a model called collaboration of multi-cloud where the user vendor lock-in can be abolished with an agreement between the various cloud service provider that an authorized user of a particular cloud service provider can gain access to different service provider as per his requirement and cost management. The main issue in implementing multi-cloud is its working in a distributed environment as the services are to be collaborated with different cloud service providers to make it possible a framework is laid in the research work of "Collaboration Framework for Multi-cloud Systems". Mixed fragmentation technique for the purpose of ensuring data privacy and confidentiality, where fragmented data has to satisfy three essential requirements before being distributed to multiple clouds are:

1. The database has to be in third normal form before any kind of process is applied, so each table can be treated as independent fragment
2. Confidentiality levels define the importance of the data contained in a fragment
3. User Requirements provide a set of additional demands concerning the distribution of the fragments that can be chosen by the user

In this paper, we proposed a concept of synthesizing the advantages of both mixed fragmentation technique in data distribution and collaboration multi-cloud model which holds an economical distribution of data among the available Service Providers in the market, to provide customers with achievable distributing merits which intern includes preserving confidentiality, integrity andavailability (CIA) perimeters by making use of multiple distinct clouds simultaneously.

2. LITERATURE REVIEW

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. The following three parameters confidentiality, integrity and availability decide whether security and privacy of data stored on cloud environment is maintained or not. Cloud computing is a distributed computing style which offer integration of web services and data centres.

Collaboration Framework for Multi cloud System:
Cloud collaboration allows clients and cloud applications to simultaneously use services from and route data among multiple clouds. This framework supports universal and dynamic collaboration in a multi cloud system. It lets clients simultaneously use services from multiple clouds without prior business agreements among cloud providers, and without adopting common standards and specifications. Multi cloud will give a review of the systems which will be useful for moving from the single cloud structural planning to multi-cloud building design, a security model and expense viability of multi-cloud contrasted with a cloud.

Uses of collaboration multi-clouds:

- Better privacy
- User data blocks
- Fragmentation of data
- Data integrity
- Dos attack
- Data intrusion / Hacked passwords

Data Fragmentation and Distribution Model:

Manipulating large amounts of data is a process that requires lots of computational resources. Facilitating efficient and fast data transport over the network is commonly ensured through one or several connections at the same time. To decrease and optimize processing costs, data in relational databases is split up into smaller pieces, which we address as fragments.

Advantages of fragmentation:

- Applications work with views rather than entire relations.
- Efficiency
- Data is stored close to where it is most frequently used.
- Parallelism
- With fragments as unit of distribution, transaction can be divided into several sub-queries that operate on fragments.

Mixed Fragmentation:

In this paper we embedded the mixed fragmentation technique in cloud, which is the Combination of horizontal and vertical fragmentations is mixed or hybrid fragmentations (MF). In this type of fragmentation scheme, the table is divided into arbitrary blocks, based on the needed requirements this type of fragmentation is the most complex one, which needs more management, in most cases simple horizontal or vertical fragmentation of DB applications. Mixed fragmentation (hybrid fragmentation) Consists of a horizontal fragment followed schema will not be sufficient to satisfy the requirements of the by a vertical fragmentation, or a vertical fragmentation followed by a horizontal fragmentation. Mixed Fragmentation is defined using the selection and projection operations of relational algebra:

$$\Pi\_p (\_A1,...,An(R))$$

$$\Pi \_A1, An (\_p(R))$$

The main reasons of fragmentation of the relations are to: increase locality of reference of the queries submitted to database, improve reliability and availability of data and performance of the system, balance storage capacities and minimize communication costs among sites.

3. CLOUD SECURITY ISSUES

The rule issues disseminated registering appearances are shielding grouping and dependability of data in helping data security. The key response for these issues is encryption of data set away in the cloud. Regardless, encryption of data in like manner raises new issues. Here is a diagram of a rate of the key issues stood up to by cloud systems and a couple of courses of action.

- **Trust:** Trust between the Service supplier and the client is one of the primary issues distributed computing confronts today. There is no chance to get for the client to make certain whether the administration of the Service is dependable, and whether there is any danger of insider assaults. This is a noteworthy issue and has gotten solid consideration by organizations. The main authoritative archive between the client and administration supplier is the Service Level Agreement (SLA). This archive contains every one of the assentions between the client and the administration supplier; it contains what the administration supplier is doing and is willing to do (Weis and Alves-Foss, 2011). In any case, there is as of now no reasonable arrangement for the SLA, and in that capacity, there may be administrations not recorded in the SLA that the client may be unconscious that it will require these administrations at some later time.
- **Legal Issues:** There are a few administrative prerequisites, protection laws and information security laws that cloud frameworks need to hold fast to. One of the significant issues with holding fast to the laws is that laws change from nation to nation, and clients have no influence over where their information is physically found. Respectability is keeping the dishonorable adjustment of data. Safeguarding Integrity, similar to secrecy is another significant issue confronted by cloud frameworks that should be taken care of, and is additionally chiefly done by the utilization of information encryption.
- **Authenticity:** In a typical database setup, there would be numerous clients with changing measure of rights. A client with a restricted arrangement of rights may need to get to a subset of information, and may likewise need to check that the conveyed results are legitimate and finish (that is, not harmed, changed or missing anything) (Weis and Alves-Foss, 2011).
- **Querying Encrypted Data**: There are several methods that were proposed to handle Querying of Encrypted Data, one such method was proposed by Purushothama B.R. and B.B. Amberker in (Purushothama&Amberker, 2013).

4. EXISTING SYSTEM

Earlier framework for generic cloud collaboration allows clients and cloud applications to simultaneously use services from and disseminates data among multiple clouds. This framework facilitates universal and dynamic collaboration in a multi-cloud system. This approach uses standard distributed techniques to share their data to customers. But here multi-cloud architecture have some security issues while collaborating the clouds such as isolation management, data exposure and confidentiality, virtual OS security and securely along with a suite of proxy services to support various collaboration methods. Thus it may lead some dissemination problems, and it yields bad results on CIA perimeters.

5. PROPOSED SYSTEM

Flexibility and simplicity are the benefits of cloud storage, but they are double-edged swords. For the tenant's outsourced data, tenants can administrate the cloud providers easily and flexibly also means that administration and operations are not controlled by the tenant. By using of multiple cloud providers for gaining security and privacy benefits is nontrivial. Data fragmentation is one of the primary techniques used in partitioning and developing cloud computing services for multi-

cloud architecture. In this paper, we proposed the mixed fragmentation scheme for multi-cloud storage in cloud computing, which provide each customer with confidentiality, integrity and availability (CIA) and also better cloud data storage decisions.

6. CONCLUSION

In these paper we briefed, how the data are stored in multi-clouds and how the security of the data is maintained along with integrity of the data .Using dynamic collaboration framework such accessing the data and the verification and security of the data is maintained within the cloud. A hybrid data fragmentation scheme for multi cloud storage in cloud computing, which seeks to provide each customer with (CIA)perimeters and better cloud data storage decisions.

7. FUTURE WORK

Currently, our research going towards a mixed fragmentation strategy based on three rules such as Completeness , Reconstruction, Disjointness to ensure trust, and safety requirements. But here we have seen some security issues while applying the rules on collaborated clouds. We are also improving data distribution threshold on multi cloud strorages. Our Incremental approach to the development of data replication Services for collaborated clouds initially provides support for Simple use cases, later progressing to more complex use cases.

REFERENCES

[1] S. M. M1. W. Itani, A. Kayssi, A. Chehab, “Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures,” Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Dec 2009.

[2] Jake Widman, 10 massive security breaches, http://www.informationweek.com/news/galleries/Security/attacks/229300675, Visited 8.11.2015..

[3] Stefano ceri Giuseppe pelagati “Distributed Databases-Principles and systems”Tata MC Graw Hill 2008.

[4] R. Thandeeswaran, S. Subhashini, N. Jeyanthi1, M. A. SaleemDurai, “Secured Multi-Cloud Virtual Infrastructurewith Improved Performance”, cybernetics and information technologies XII, (2), pp. 11-22, 2012

[5] MukeshSinghal and Santosh Chandrasekhar, Tingjian Ge, Ravi Sandhu and Ram Krishnan, Gail-JoonAhn, andElisaBertino “Collaboration in Multicloud Computing Environments: Framework and Security Issues”, Published by the IEEE Computer Society IEEE, 2013.

[6] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, “On Technical Security Issues in Cloud Computing,” Proc. IEEE Int’l Conf. CloudComputing (CLOUD-II), 2009.

[7] P. Mell and T. Grance, “The NIST Definition of Cloud Computing,Version 15,” Nat’l Inst. of Standards and Technology, InformationTechnology Laboratory, vol. 53, p. 50, http://csrc.nist.gov/groups/SNS/cloud-computing/, 2010.

[8] Mohamed Almorsy, John Grundy, and Amani S. Ibrahim, “TOSSMA: A Tenant-Oriented SaaS Security Management Architecture”, 5th IEEE Conference on Cloud computing IEEE, 2012.

[9] P. F. Oliveira, L. Lima, T. T. V. Vinhoza, J. Barros, M. M´edard,“Trusted storage over untrusted networks”, IEEE GLOBECOM 2010, Miami, FL. USA.

[10] M. Armbrust, A. Fox, R. Grifth, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the clouds: Aberkeley view of cloud computing. Technical re-port, University of California at Berkeley, February 2009.