Quality Aspects and Challenges In Collaboration of Multi-Cloud - A Study

Swetha D. M.tech (Scholar)
Dept.of CS&E, VTU, PG centre, MYSORE
Karnataka (State) ,India

Dr. Thippeswamy K. Professor & Head
Dept. of CS&E,VTU, PG centre, MYSORE
Karnataka (State) ,India

Abstract **- Collaboration among services or application offered by different clouds is still restricted , the adoption of these technology will improve the ease of access from one provider to another and increase open challenges which avoid the vendor lock-in issues. As the number of services and providers are increasing, the complexity of the overall system and the number of potential attacks will also increase. Preserving the security among multi-cloud is very important and trust among the providers is essential as the user often store sensitive information in cloud. Different providers will have different security rules or different protocol standards, making it complex to monitor security policies in composite services. In this paper we discuss the quality aspect related to the security issues by considering areas such as privacy, integrity, authentication, availability.**

Keywords **-** ***Multi-Cloud, Security, Quality prediction, Availability***.

1 INTRODUCTION

The cloud computing is a culmination of numerous attempts at large scale computing with seamless access to virtually limitless resources The term cloud computing should not end with the single cloud .Cloud collaboration is a newly emerging way of sharing and co-authoring computer files through the use of cloud computing, whereby documents are uploaded to a central cloud for storage, where they can then be accessed by others. Cloud mashups are recent trend[1]. Mashups combine services into single application. In the last few years industries have been increasingly switching to use of cloud collaboration..Many services are collaborated from multiple clouds (or multi-cloud environments) in to a single application which avoid the risk of vendor lock in. New technologies and standard have been developed to support the collaboration of multi-cloud. The adoption of standards and technologies will improve the ease of access from one provider to another. The data related aspects are relevant for interoperability since only two or more services offering mechanisms to guarantee global data properties might be combined in the same application.

For instance, the service delivery model requires user to register to a service. Because of this, a service in a certain CSP will not allow user from other CSPs to use it without going through the necessary service level agreement or registration process. This adds complexity to the collaboration. In collaboration of multi-cloud environment several factors to be included to avoid the risk such as privacy, integrity, availability. The use of services from multiple cloud service providers adds a complexity to an already complex cloud computing scenario. Heterogeneity of services caused by the existence of different providers have created their own models, protocols, standard, processes and formats must be taken into account which will lead to the increase in the number of risks when creating a new application or services using a multi- cloud strategy. the factor included both functional and non functional measures as well as the cost and added value

Many industries buying cloud computing services neither know nor care about where the processing power comes from, nor how the computing capability is put together. The users do care about is the capacity of cloud computing to introduce significant new levels of scalability and flexibility, including: Lower infrastructure, maintenance and energy costs ,Pay-per-use capacity as the business needs it, with the flexibility to scale the service and price up and down to handle unexpected load changes, Accelerated speed to market

In this paper discuss about the risk and quality aspect that are specific to the multi-cloud environment. They are two important factors that are to be considered which are essential in multi-cloud environment:1) Interoperability of services or migration from single cloud to multi-cloud to avoid vendor lock-in .2) Security issues such as privacy, integrity, availability etc..

2 LITERATURE REVIEW

J Suresh Babu et.al [2] has a review that the term cloud computing should not mean single cloud but also include multi-cloud. All the problem that are faced by single cloud can be addressed by using multi-cloud. They focused on the issues related to the data security aspect of cloud computing. As the user often store sensitive information or the data in the cloud storage but this providers may be not trusted and possibility of malicious insider in single cloud so this paper surveys to shift from single cloud to multi-cloud. The cloud providers must be give high priority to the data privacy and security issues.

Victor Muntés-Mulero and Peter Matthews et.al [3]. has a review that , as the concept of multi-cloud has evolved ,risk and quality of multi-cloud should be give importance. They analyze three important factors such as interoperability , migration from current service to a new equivalent service, and the security issues that arise from the privacy, integrity, availability, etc. Risk are analyzed based on the quality aspects such as 1)Risk of unexpected lack of replacement and consequent vendor lock-in, 2)Risk of new security breaches due to the increased complexity of the system and new communications.3) Risk of non-viable migration due to migration costs and complexity. 4)Risk of lack of provider interest in collaboration. Some essential aspects to establish the necessary baseline for a decision support method aimed at facilitating the selection of cloud services and providers in a multi-cloud environment.

Monali Shrawankar et.al. [4] has a review that it will guarantee to prevent security risk by providing a secure cloud database. In this framework they concentrated on data intrusions ,data integrity and service availability in multi-cloud.and they present a virtual storage cloud system called DepSky which consists of combination of different clouds to build a interclouds. In this DepSky model ,locations the accessibility and the confidentiality of data in their storage system by using multi-cloud providers, blending Byzantine quorum scheme protocols, cryptographic secret sharing and erasure ciphers.

3.SPECIFIC NEED AND CHALLENGESIN MULTI-CLOUD ENVIRONMENT

Characterization Of Quality Aspect In Multi-Cloud

The characterization of quality in multi-cloud environment is based on different factor such as interoperability issues, ease of migration in multi-cloud environment and the security issues.

3.1.1 Interoperability Issues.

Interoperability of one cloud service provider to another cloud is very important to make customer to except more from cloud computing. and without standardization interoperability of specific application and service functionality from one cloud to another is impossible and it restrict the implementation causing instability in area such as security[5]. The Technical interoperability quality aspects refer to the capacity of two or more services offered by different providers to communicate through common protocols and to jointly guarantee a certain quality of service. From the developer point of view, it is important to know the degree of interoperability of a certain service with respect to other service. Table 1 shows the Quality aspects and indicators for interoperability in multi-cloud systems

TABLE 1 Quality Aspects And Indicator For Interoperability In Multi-Cloud System

Interoperability	**Specific aspects**	**Indicator**
Technical	Compatible quality of service	-Average recovery time -Uptime, response time,
Semantic	Data quality	-Data completeness - Data consistency - Relevance of data
Industry	Working process compatibility	Number of functionalities similar to other services of the same type offered by other providers

3.2 Ease of migration in multi-cloud environment

Migration is an essential operation in multi-cloud environments. If the services interacting with cloud database service assume that these tools exist, moving to a new cloud database that does not provide these tools will require reengineering part of the system and it may lead to too expensive .Export and import migration setup can be indicated by considering number of proprietary configurations based on a standard format.

3.3 Security Issues

Preserving security in a multi-cloud environment is important and trust among the different cloud service providers is essential as user store sensitive information in the cloud .security issues is based on factor such as privacy, integrity availability, authentication and authorization etc.

3.3.1 Privacy or Confidentiality

As the services are collaborating , privacy of the data is very important because there a movement towards different service providers so there must be service agreement(SLA) or terms and condition to be applied so that user of another cloud service provider should not change the data or information.

SLA - Service Level Agreements play a central role in the service lifecycle. SLAs are agreements limited to description of expectations and responsibilities. An SLA cannot guarantee that user will get the service it describes, At the same time, an SLA can mitigate the risk of choosing a bad service. Service is delivered according to specific quality levels. Enforcing SLAs when dealing with different transactional cloud is very important. So cloud service provider should' not break the term and condition .At last the adoption of current SLA standards highlights the success potential and need for standards.

3.3.2 Integrity

The data stored in the cloud may be corrupted or damage during transition operations from or to the cloud storage provider. Maintaining consistency of data is very important.. If the more the number of times file corrupted for client are higher, then it concludes that the authentication of the user has a damage and his documents are purposely corrupted by

compromise of authentication parameters so there must be Level of agreement between CSPs on mechanisms for data integrity preservation.

3.3.3 Service Availability or High Availability

Another major concern in collaboration of multi-cloud is service availability. Amazon didn't not assure the user that they will provide the services all the time in the SLA. The user‘s web service may terminate for any reason at any time if any user‘s files break the cloud storage policy.

Service availability in multi-cloud can be guaranteed by maintaining the backup copy in another clouds so that if one cloud is down , the data can be retrieved from another cloud in this way user will get services on all. time, the backup copy or replication must be done in minimum of two cloud. As a service is replaced all data related to that service should be archived.

3.3.4 Authentication and Authorization

Another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. Someone gains access to password; they will be able to access all of the account‘s instances and resources**.** if client authentication is hacked and fakes user can login and can corrupt the data. So there must be proper authentication and authorization must be provided. The adoption of grades of security for the client is needed if client data is corrupted .the user can be moved to the largest security profile . biometric authentication is more secure than the user title password founded authentication.

Another security risk that may occur with a cloud provider, such as the Amazon cloud service, is a hacked password or data intrusion. Someone gains access to password; they will be able to access all of the account‘s instances and resources**.** if client authentication is hacked and fakes user can login and can corrupt the data. So there must be proper authentication and authorization must be provided. The adoption of grades of security for the client is needed if client data is corrupted .the user can be moved to the largest security profile . biometric authentication is more secure than the user title password founded authentication.

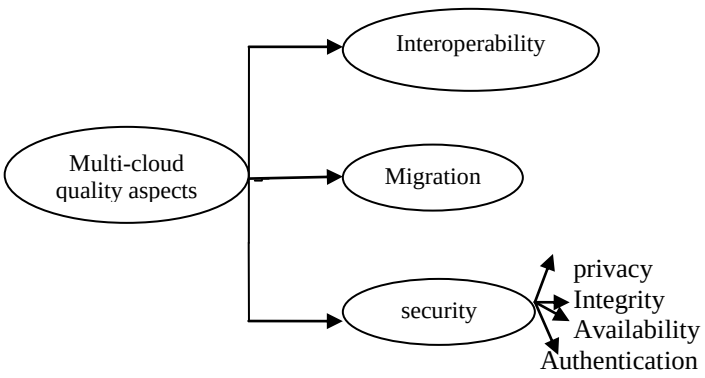

Fig 1: Quality Aspects in Collaboration of Multi-Cloud Environment

4 SPECIFIC RISK AND COST IN MULTI-CLOUD ENVIRONMENT

The risks are based on analysis of quality aspects that make multi-cloud environments independent from clouds provided by a single provider. Independent providers use proprietary interfaces and configurations. Services are also highly integrated with lower-level services offered by the same CSP. Examples of this may be lack of common SLA , use of non-compatible technologies, lack of compatibility in the communications protocol, lack of shared mechanisms to ensure data consistency and quality, the existence of services which are not strictly equivalent and miss some important functionalities.

Lack of provider interest in collaboration are risk in multi-cloud environment. Service level agreements are usually required for two CSP to collaborate. For instance, if the service delivery model requires customers to register to a service. Because of this, a service in a certain CSP will not allow customers from other CSPs to use it without going through the necessary registration process, unless the right agreements are put in place. Besides, vendors may try to retain customers at any cost to be more competitive. Contracts and other legal issues made the user to make it difficult to migrate from one service to an equivalent one. In other words, there is a risk of unfair customer retention and consequent vendor lock-in.

Another essential factor in multi-cloud environment is cost . Migration from one service to another will lead to more economic cost that must be considered at the design time. Cost include hardware and resources necessary for migration and the cost of training the users of the application.

5 CONCLUSION

Vendor lock-in is major drawback in cloud computing environment, this can avoided by collaborating different providers. Several factor are included while collaborating the services because independent providers will have different standards and configuration and user expect the services from the cloud all the time(High availability). Providing security to the cloud is very essential. This paper surveyed on quality aspect and challenges in multi-cloud environment such as Interoperability, Security, ease of migration which is much necessary when collaborating multi-cloud

6 ACKNOWLEDGEMENT

I would like to thank the Department of computer science & Engineering, VTU University, VTU PG centre, Regional Office, Mysore for providing support to conduct this research work.

REFERENCES

[1] Mukesh Singhal and Santosh Chandrasekhar, Tingjian Ge, Ravi Sandhu and Ram Krishnan, Gail-Joon Ahn, and Elisa Bertino "Collaboration in Multicloud Computing Environments: Framework and Security Issues", Published by the IEEE Computer Society IEEE, 2013

[2] J Suresh Babu, K Kishore, K E Naresh Kumar " Migration from Single-Cloud to Multi-Cloud Computing" April 2013,Volume 2, Issue 4.

[3] Victor Muntés-Mulero and Peter Matthews, Aida Omerovic, Alexander Gunka "Eliciting risks, Quality and Cost aspects in Multi-Cloud Environment"' Page 238-243

[4] Monali Shrawankar , Ashish Kr. Shrivastava"Security Threat Solution over Single Cloud To Multi-Cloud Using DepSky Model" volume 14 Issue 1 page 71-76, sep-oct 2013.

[5]. S. Ortiz Jr., "The Problem with Cloud Computing Standardization," *Computer*, July 2011, pp. 13-16.

[6] MODA CLOUD Grant Agreement N° FP7-318484 http://www.modaclouds.eu/