Eliciting Risk, Quality and Cost Aspects in Multi-cloud Environments

Victor Muntés-Mulero and Peter Matthews
CA Technologies
CA Labs Europe
Email: {Victor.Muntes, Peter.Matthews}@ca.com

Aida Omerovic
SINTEF
Oslo, Norway
Email: aida.omerovic@sintef.no

Alexander Gunka
BOC Information Systems
Austria
Email: alexander.gunka@boc-eu.com

***Abstract*—With the increasing number of providers offering cloud-based services, new opportunities arise to build applications capable of avoiding vendor lock-in issues. Such applications are developed in multi-cloud environments that allow replacing services with those offered by alternative providers. While this may improve quality and provide independence from a single cloud service provider, it also brings new risks. Being able to assess risks and those quality aspects that are specifically related to multi-cloud environments is essential in order to design reliable applications based on the use of cloud services. Although a lot of work has been done to study risks and quality aspects for cloud services, this is usually focused in single-provider scenarios. In this position paper, we discuss several risks and quality aspects that are specifically related to multi-cloud environments.**

Keywords- Multicloud, Risk assessment, Quality prediction, Cost prediction

I. INTRODUCTION

Many applications and Cloud Service Providers (CSPs) replicate or combine services from multiple clouds or multi-clouds (also called cloud mashups [9]) to avoid the risk of vendor lock-in. New architectures, technologies, and standards are being proposed to support collaboration among multiple cloud systems [1], [2], [6], [7]. Although direct collaboration among applications hosted by different clouds is still restricted [9], the adoption of these proposals will improve the ease of migration from one provider to another and increase open competition. Nevertheless, the current environment already offers many opportunities for collaboration among services offered by different providers without requiring standards or important changes to the delivery model.

In multi-cloud environments, it is essential to provide tools that guide multi-cloud application architects to choose the services providing the necessary quality and ensuring acceptable level of risk. Previous work has focused on describing quality aspects and metrics to measure the suitability of a cloud service from a multi-dimensional perspective. An example of this is the Service Measurement Index (SMI) [10], a framework designed to allow for quick and reliable comparison of IT business services. SMI establishes the basis for comparing isolated services in regard of several categories such as for instance accountability, agility or assurance. However, they do not explicitly analyze these aspects in a multi-cloud context.

Based on this quality aspects and other factors, model-based decision making system help application designers to choose the cloud components that better fit their needs. Some of these major factors include functional and non-functional properties, as well as cost and the added value. A trade-off between such factors is the basis for decision making. This trade-off is particularly complex between the non-functional factors, the variable parts of the architecture, and the cost of the selected solutions. The variability, as well as incomplete information or knowledge, are also sources of risk. Since functional requirements are less flexible and specified rather early, and since the added value is strongly related to functional properties, the factors that are tuneable and highly interrelated are risk, quality and cost.

In this paper, we discuss the risks related to cloud services in a multi-cloud environment, the quality aspects that are specific to that environment and make some cost considerations. We analyze three important issues which are essential in multi-cloud environments: interoperability issues between services offered by different providers, the ease of migration from a current service to a new equivalent service, and the security issues that arise from the fact that confidentiality, integrity, availability, etc. does not depend on a single provider.

This paper is organized as it follows. Section II presents related work. Section III briefly describes multi-clouds escenarios and describes the aspects considered in this paper. Section IV presents a summary of quality aspects to be considered. Section V provides a brief description of costs that must be taken into account in this type of environment. In Section VI, we discuss risks that must be considered in a multi-cloud. Finally, Section VII presents the conclusions and draws some future work.

II. RELATED WORK

As a basis for the elicitation of the adequate quality characteristics, the software product quality standard ISO/IEC 9126 defines quality as the totality of features and characteristics of a software product that bear on its ability to satisfy stated and implied needs. The ISO 9126 standard provides an established specification of decomposed quality notions with their qualitative and quantitative definitions. The standard defines a quality model for external and internal quality, and for quality in use. The characteristics of the internal and external quality model are functionality, reliability, usability, efficiency, maintainability and portability. These are in turn decomposed into a total of 34 sub-characteristics.

SMI [10] is a standardization effort from the Cloud Services Measurement Index Consortium (CSMIC) consisting of

 ISBN: 978-1-61208-271-4

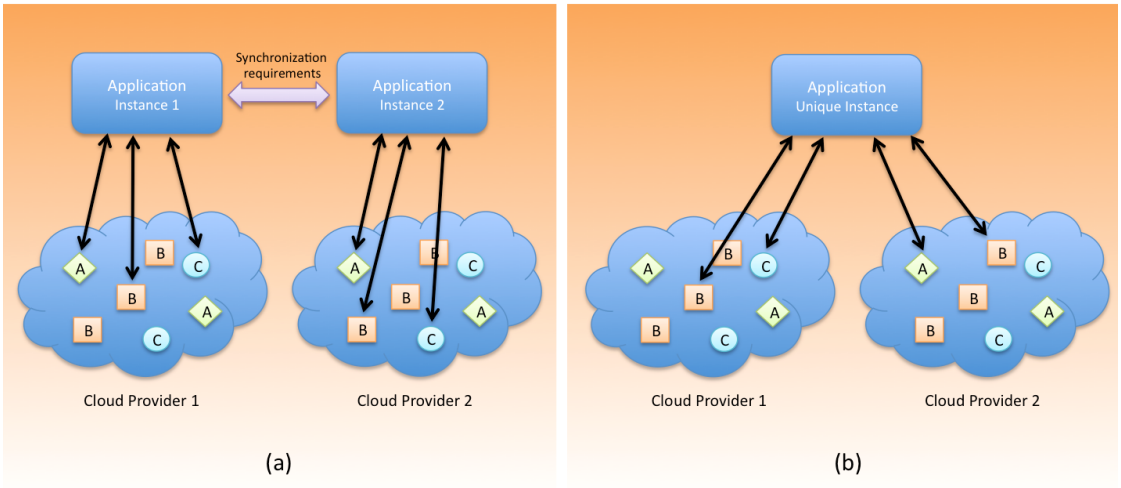

Fig. 1: Examples of two different multi-cloud scenarios

academic and industry organizations. The Service Measurement Index (SMI) uses a series of characteristics and measures to create a common means to compare different services from different suppliers. The characteristics are categorized as Usability, Performance, Agility, Security and Privacy, Financial, Assurance and Usability. Each of these characteristics has a number of measures that can be used to evaluate the risk in using a service. For example in the accountability category one of the measured attributes is Compliance and another is Service-Level Agreements (SLA) verification both of which can be used to create a risk measure for the service and the provider. The work presented in this paper is based both on the ISO standard and SMI conclusions.

In order to enable risk monitoring based on indicators or metrics, there is a need not only to identify the relevant indicators, but also to understand how to relate the indicators to potential risks, and how to aggregate the monitored values into risk levels [5]. In this paper, we identify both risks and quality aspects related to multi-cloud environments. To our knowledge, none of the previous work has been focused on jointly analysing risk, quality and costs in a multicloud environment.

III. MULTI-CLOUD SPECIFIC NEEDS AND CHALLENGES

We define a *multi-cloud application* as any piece of software using several cloud services hosted by two or more different providers. Usually, two different scenarios are considered when referring to multi-cloud environments. Figure 1 depicts these two cases. In the first case (a), an application is replicated to improve resilience, and may also be used to avoid vendor lock-in. This means that the application has two independent instances using the same type of cloud services (A, B, C in the figure) in two different cloud providers. In the second case (b), a single instance of the application runs different cloud services hosted by two or more cloud providers. In this latter case, it is also possible to replicate services to ensure availability. This would also imply synchronization. Because of the need for high interoperability between services offered by different providers, scenario (b) is in general more complex to manage and may potentially involve larger risk compared to (a). In fact, scenario (a) may be considered a particular case of scenario (b). Because of this, we focus on scenario (b) in this paper.

The use of multiple cloud services from multiple providers adds a new dimension of complexity to an already complex cloud computing scenario. Heterogeneity caused by the existence of independent providers that have created their own business models, protocols, processes and formats generates an increasing number of risks to be taken into account when creating a new application using a multi-cloud strategy. In this paper, we emphasize three essential aspects that must be considered in a multi-cloud environment:

- **Heterogeneity of services offered by different providers results in reduced interoperability**: the lack of standard interfaces for services in different clouds and the creation of independent proprietary systems by each provider, make multi-cloud environments very heterogeneous. Interoperability problems may range from technical issues, such as messaging interfaces or quality of service, to semantic, organizational or legal issues. This heterogeneity is an important risk to consider at design time, since it will influence the capacity of an application architect to decide between one service and another. In terms of quality, a service will be highly interoperable with other systems if it can be combined in collaboration with many other services, from the same or other cloud service providers.
- **Migration between services offered by different CSPs is an essential operation to ensure the compliance with the application requirements**: one of the most common reasons to deploy an application in a multi-cloud environment may include increasing the cloud service catalog and increasing the capacity of users to migrate from one service to another in case the requirements on the application are not fulfilled. We call this capacity *replaceability*, and it represents the ease to migrate from one service to another to replace the first one. It will be essential to decompose migration processes from one cloud service to another into several finer-grained steps, and analyze the quality

 ISBN: 978-1-61208-271-4

aspects to be considered in the process.

- **Security threats are increased in multi-cloud computing environments**: increasing the number of services and providers, will increase the complexity of the overall system and the number of potential attacks. Control over customers data decreases, especially because of potential migration between services of different providers. The continuous communication of data between services in different clouds may also result in storing data in intermediary less secure external storage systems, increasing the overall vulnerability and potentially compromising confidential information. In terms of data privacy, multitenancy makes it more difficult to guarantee confidentiality of sensitive information.

These three aspects have been selected and prioritized after several interviews with industrial and academic partners. They have been chosen based on experience and from studying different migration processes. They represent three essential requirements in a multi-cloud environment: coordination between services offered by different providers, capacity to replace a service by another one, and the increase of complexity in the system increasing possible points of failure in terms of security. Note that, we do not claim this to be a comprehensive list of possible aspects to analyze, but we believe they are a good starting point to establish the basis to define risk and quality in multi-clouds.

IV. Quality Aspects in Multi-Cloud Environments

In this section, we analyze those quality aspects related to the issues detected in Section III that must be considered in a multi-cloud environment: interoperability, replaceability and security. Figure 2 summarizes the quality aspects considered related to these three issues.

A. Interoperability

The interoperability problems of cloud services in the controlled environment of a single CSP, are exacerbated by mixing services from different providers and may imply incompatibilities in other areas of a mixed service implementation. From the point of view of a developer, it will be important to know the degree of interoperability of a certain service with respect to other services it must interact with. Figure 3 depicts the scenario studied in this case. Figure 2 divides these incompatibilities in four different areas: technical, semantic, organizational and legal. 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. For instance, possible indicators that might be used to evaluate the degree of technical interoperability might be the number of standardized interfaces that can be compared towards the total number of interfaces used by the service, or the average recovery time of the service or other performance aspects. Semantic aspects refer to aspects related to the data syntax consistency and the data quality. These 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. Organizational aspects

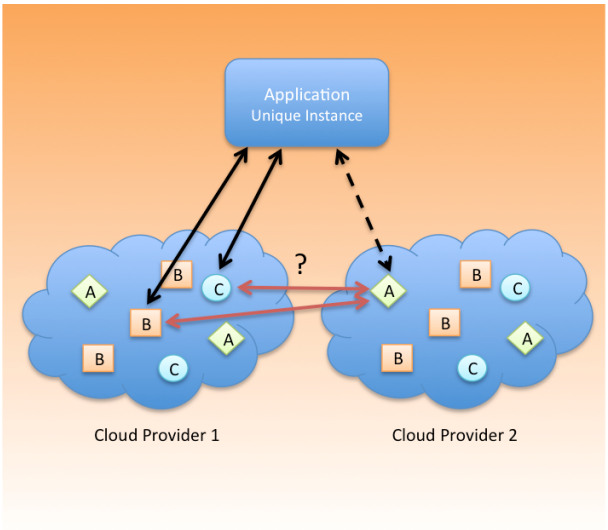

Fig. 3: Interoperability in a multi-cloud environment: services offered by different providers interacting with each other.

indicate how adaptable a service is to several work processes. Since each of these work processes might be established by different providers, it is important that a service in a multi-cloud environment is adaptive to fit the requirements of each work process in each case. Changes in a work process may require changes in a specific cloud service that is already used. In a migration process, choosing a new cloud service candidate to replace an existing service may depend on the capacity of this new service to adapt to the existing work process. Compliance with existing cloud service standards in terms of role and functionality of that specific cloud service will be essential to ensure good organizational interoperability. Regarding legal aspects, we focus on regulatory compliance. Compliance in this case may be understood as a list of laws that are observed by the service provider. Some may be mandated by the customer such as Sarbanes-Oxley [8], some by government, e.g. Data Protection act [3]. It is the presence or absence of compliance that is of interest. A purchasers compliance officer will provide a number of regulations that any service would have to observe and these would be part of the requirements gathering.

Several aspects are likely to be difficult to measure. A good example is the number of standards in the communication capability aspect. Standards for cloud service communications are evolving and several attempts have been made to create an agreed list of them. NIST has a list of recommended standards and the European Commission has created a Cloud Standards Coordination (CSC) that is being administered by ETSI [4]. The requirements of multi-cloud applications may need some or all of the relevant standards to be adhered to.

B. Intercloud Replaceability

Migration is an essential operation linked to multi-cloud environments. The capacity of a software architect to redesign an application and replace existing services by other services with the same or similar functionalities defines in fact the realism of considering cloud mashups. For instance, a cloud database service may integrate application building tools that

 ISBN: 978-1-61208-271-4

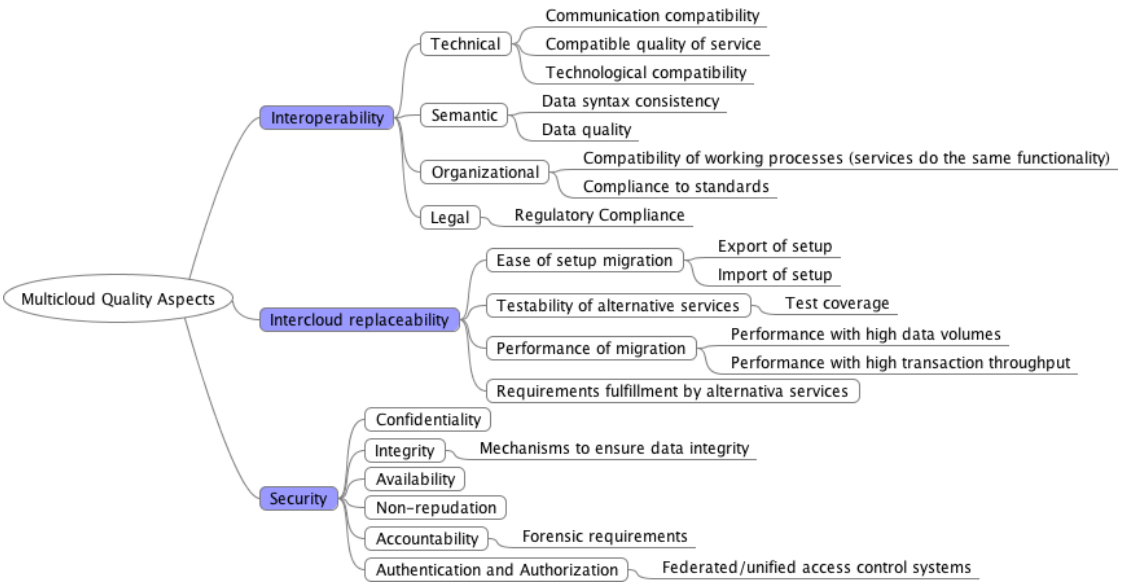

Fig. 2: Quality aspects related to multi-cloud environments

might be used by our system, such as APIs based on web services standards. If the other services interacting with this cloud database service assume that these tools exist, moving to a new cloud database that it does not provide these tools will require reengineering part of our system and it may have an unaffordable cost. In this subsection, we define and analyse the migration process to find the quality aspects that make a service easy to migrate from. We focus on the case where a service is replaced by one or more services offered by a different cloud provider. We consider two situations:

- The current cloud service does not fulfill the requirements of the system: this may happen for instance when the service is updated or modified, when the amount of information handled by the application grows making it impossible to comply with certain pre-established SLAs, etc. Usual examples may range from a variation in the cost that makes the service not competitive compared to other services of the same type, to a change in policies and functionalities that affects security, availability, resilience, or any other important aspect.
- The requirements of the system have changed: one or more cloud services may not fulfill these new requirements and need to be replaced.

Figure 4 depicts a generic process of service-to-service migration. First, a cloud service is selected for migration. Depending on the reason for migration, it may be necessary to review the requirements defined at design-time. After this, one or more new candidate cloud services must be selected. In order to simplify this step, Figure 4 considers a single candidate in the process. Once we have found a candidate target service to migrate to, we can export both data and the configuration from the original service. At this point, it is usually necessary to enter an intentional contract with the new service provider. In some cases, it will be also necessary to inform the old service that we are initiating a process to retire it. In this situation, the old service and the new one may be active at the same time during the testing and training process. This will depend on the availability requirements of the application migrating one of its cloud-based components. In the next step, it is important to adjust or define a new workflow for the application. This might be necessary if the new service is not perfectly compatible with the old one or if the application was redesigned in a way that the workflow was altered. After this, we can start preparing the testing environment and the new service. Usually, the testing process will be divided in several phases.

In general, it is necessary to carry out functionality and performance testing in a test environment. In this situation, data needs to be kept synchronised. Following successful functionality and performance testing, the service may move to a modification of A/B testing so that the application is tested with the new service in production before switching over completely. In case requirements are not satisfied, we must start the process again. If they are fulfilled, we can start the users training process and eliminate the old service if this is still active. Once this has been done, the application can be deployed again using the new cloud service.

Figure 2 shows several quality aspects related to replaceability. Possible indicators of quality related to intercloud replaceability may include the number of proprietary configurations that can be exported or imported based on a standard format, completeness, precision and relevance of tests, time required to migrate large amounts of data, etc.

C. Security

Preserving security becomes more complex in a multi-cloud environment. Trust among the different cloud service providers is essential. It is difficult to handle the heterogeneity of the different security rules established by each provider, making it complex to monitor security policies in composite services. Besides, an additional challenge involves data and identity privacy preservation when several services from different providers collaborate.

 ISBN: 978-1-61208-271-4

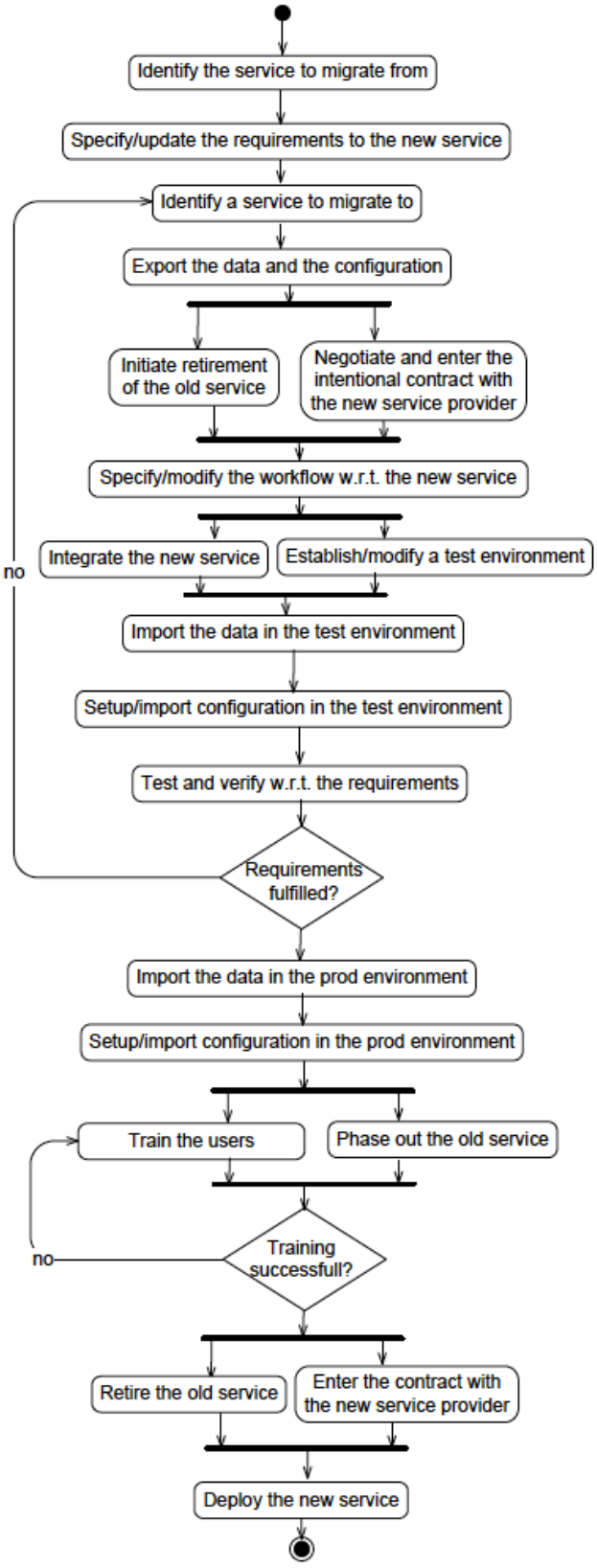

Fig. 4: Description of a generic migration process

In Figure 2, we classify quality aspects related to security in the usual areas: confidentiality, integrity, availability, non-repudiation, accountability and authentication and authorization. In order to preserve data privacy, it is crucial to establish agreements with other providers on the level of privacy of data and identities. Trust in general must be guaranteed by explicit agreements or shared protocols between providers. An alternative solution involves using reliable proxies for communication, but services still need to be able to establish agreements on the fly and secure delegation with these proxies. Finally, it will be important to evaluate services depending on the need to store data in public storage system in order to share this data with other services. In this case, data are exposed to a larger number of threats

V. COST IN MULTI-CLOUD ENVIRONMENTS

Besides risk and quality, we consider another essential dimension: cost. SMI and other previous proposals describe cost-related aspects in cloud computing environments. In a multi-cloud environment, an extra cost appears that may be also considered in the decision-making process: the cost of migration. Migrating from one cloud service to another may involve several economic costs that must be considered at design time. These costs may depend on the personnel involved in the migration process, the cost incurred by keeping the old and the new cloud services running in parallel during the migration process, the cost of the hardware or other resources necessary to perform the migration, or the cost of training the users of the application (note that this cost is also necessary in other situations, but it is usually unavoidable in a migration process).

VI. SPECIFIC RISKS IN MULTI-CLOUD ENVIRONMENTS

In this section, we sketch a list of possible potential risks that may be found in a multi-cloud system. These risks are based on the analysis of the elicited quality aspects that make multi-cloud environments different from clouds provided by a single provider.

1) Risk of unexpected lack of replacement and consequent vendor lock-in: a certain cloud service may not fulfill requirements, or requirements may change. In this situation a different service may be needed but it may not be possible to find a new service provided by another vendor which is interoperable with the other services of the system. Two theoretically equivalent services might differ in several relevant aspects. The heterogeneity between different CSPs is usually high as they typically 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 enforcement systems, 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, or the lack of services compliant with certain regulations. If this problem appears and the need for migrating from the original service is real, this may even force the migration of other services apart from the service which is not compliant with requirements.

 ISBN: 978-1-61208-271-4

2) Risk of new security breaches due to the increased complexity of the system and new communications: data needs to flow from one service to another, hosted by different providers. This creates new points of failure and potential security issues. For instance, this may be caused by the lack of shared security protocols and data integrity mechanisms, lack of forensic mechanisms to be compliant with regulations, the lack of shared authentication systems, etc.

3) Risk of non-viable migration due to migration costs and complexity: a developer may not be aware of the cost and complexity of migrating from a certain service chosen to be part of the application to other similar services (see Figure 4). This might become a risk if it is necessary to migrate from that service to another one. As we have discussed, a usual problem in a migration process is the lack of compatible data formats, making it necessary to perform transformations that require time and resources. A related problem might be the lack of information of the new service regarding a certain quality aspect. In this case, uncertainty may also impact a migration process negatively. Note also, that a technical aspect to be considered is whether two services are implemented using the same technology, which might also be a blocking factor for a fast and easy migration. Complexity in the setup migration may also be an important problem. Beyond compatibility in terms of data storage and access, the configuration of a cloud service may also be essential to guarantee the compliance with user requirements. An excessively complex migration of configurations between two services may also result in a time-consuming and expensive migration process. Besides, ease of testing a service and total downtime are two aspects that may largely impact the suitability of a certain migration. Several possible methodologies may be used for developing and support this testing. For instance, modified A/B may be used where only one service is changed and a number of different grades of testing are performed. Finally, depending on the requirements of the application, it might be necessary for the two cloud services, the original one and the replacement, to coexist during a certain period of time, during the testing process of the migration. Complexity to synchronize data between the two services might make the coexistence difficult and using the new service as a hot backup of the first is inefficient.

4) Risk of costs unpredictability: by using services from different providers, it may become more and more complex to predict costs.

5) Risk of lack of provider interest in collaboration: business agreements are usually required for two CSP to collaborate. For instance, 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 may be blockers 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.

6) Risk of unavailability of evidences in case of fraudulent actions: this is a potential risk that may be caused by the lack of forensic tools and global tracking mechanisms.

7) Risk of lack of negotiation on SLAs: large organizations using a single supplier can negotiate terms. SMEs or companies using multiple services from multiple vendors are unlikely to have the power or the time to negotiate. This will create an increasingly unstable cost and terms and conditions problem.

Note that a more formal risk analysis might be performed to consider this a final list of risks.

VII. Conclusions and Future Work

In this position paper, we have discussed 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. In particular, we argue that risk, quality and cost are among the main factors in such a selection process. We believe that a trade-off analysis between risk, cost and quality based on a consolidated view of the three will provide a useful basis for a decision maker in assessing the possible choices through a cost-benefit analysis. For this, we have reported the results of an elicitation of the risk, cost and quality aspects that are specific to multi-cloud environments. We argue that security, interoperability and ease of migration are among the main quality aspects in a multi-cloud environment.

Beyond this initial analysis, we plan to develop a comprehensive study on risk and quality aspects to be considered in a multi-cloud. With this, we aim at creating a decision support tool able to help multi-cloud applications architects to design their systems. This tool will be implemented based on a new methodology that integrates risk, quality and cost dimensions.

Acknowledgment

This work has been conducted as a part of the MODAClouds project (Grant Agreement FP7-318484) funded by the European Commission within the 7th Framework Programme.

References

[1] D. Bernstein and D. Vij, Intercloud Security Considerations, Proc. 2nd Intl Conf. Cloud Computing (CloudCom 10), IEEE Press, 2010, pp. 537-544.

[2] R. Buyya et al., Market-Oriented Cloud Computing: Vision, Hype, and Reality of Delivering Computing as the 5th Utility, Proc. 9th IEEE/ACM Intl Symp. Cluster Computing and the Grid (CCGRID 09), IEEE CS, 2009, pp. 599-616.

[3] Data Protection Act 1998. http://www.legislation.gov.uk/ukpga/1998/29/contents

[4] European Telecommunications Standards Institute (ETSI). http://www.etsi.org

[5] Ligaarden, O. S.: A Framework for Analyzing and Monitoring the Impact of Dependencies on Quality. PhD thesis, University of Oslo (2013)

[6] M.P. Papazoglou and W. van den Heuvel, Blueprinting the Cloud, IEEE Internet Computing, Nov./Dec 2011, pp. 74-79.

[7] B. Rochwerger et al., ReservoirWhen One Cloud Is Not Enough, Computer, Mar. 2011, pp. 44-51.

[8] Sarbanes-Oxley Act of 2002 (Pub.L. 107204, 116 Stat. 745, enacted July 30, 2002). http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/html/PLAW-107publ204.htm

[9] Singhal, M.; Chandrasekhar, S.; Tingjian Ge; Sandhu, R.; Krishnan, R.; Gail-Joon Ahn; Bertino, E., "Collaboration in multicloud computing environments: Framework and security issues," Computer, vol.46, no.2, pp.76-84, Feb. 2013

[10] Cloud Services Measurement Index Consortium: CSMIC Website http://csmic.org/. Accessed, March 2013

 ISBN: 978-1-61208-271-4