A Risk Assessment Framework and Software Toolkit for Cloud Service Ecosystems

Karim Djemame
School of Computing
University of Leeds
Leeds, UK LS2 9JT
scskd@leeds.ac.uk

Django J. Armstrong
School of Computing
University of Leeds
Leeds, UK LS2 9JT
een4dja@leeds.ac.uk

Mariam Kiran
School of Computing
University of Leeds
Leeds, UK LS2 9JT
scsmk@leeds.ac.uk

Ming Jiang
School of Computing
University of Leeds
Leeds, UK LS2 9JT
scsmj@leeds.ac.uk

***Abstract*—As the realization of Cloud computing environments advances from a simple and single private Cloud towards a more complex Cloud Service Ecosystem consisting of multiple coexisting public or hybrid Clouds, there are emerging high level concerns such as risk, trust, ecological, security, cost and legal factors that underpin the non-functional properties of the ecosystem. These concerns are beyond the traditional focus of providing functionalities at levels close to a single Cloud infrastructure such as hardware resource virtualization. In this paper we present ongoing research work to analyze and address the risk factor in such a Cloud Service Ecosystem for the purpose of optimizing Cloud service. The main contributions of the work are the design and implementation of an effective and efficient risk assessment framework (methodologies of risk identification, evaluation, mitigation and monitoring) for Cloud service provision. Together with the corresponding mitigation strategies, the framework provides technological assurance that will lead to a higher confidence of Cloud service consumers on one side and a cost-effective and reliable productivity of Cloud Service Provider (SP) and resources organized by individual Infrastructure Provider (IP) on the other side. The design of the risk assessment framework and its software toolkit implementation is part of the research and development work of the OPTIMIS (Optimized Infrastructure Services) project whose objective is to enable an open and dependable Cloud Service Ecosystem that delivers IT services that are adaptable, reliable, auditable and sustainable both ecologically and economically.**

Keywords-risk assessment; Cloud services; service provider; infrastructure provider; optimization.

I. INTRODUCTION

The current model of a single Cloud service infrastructure mainly focuses on providing functionalities at levels close to the infrastructure, e.g., improved performance for virtualization of all, compute, storage, and network resources, as well as necessary raw functionality such as virtual machine migrations and server consolidation. However, for a Cloud Service Ecosystem that consists of multiple coexisting Cloud architectures, there are higher level concerns (e.g., risk, trust, ecological and legal factors) that should be addressed for the purpose of an optimized Cloud service provision. The purpose of this research work is to analyze and address the risk factor in a Cloud Service Ecosystem. Although in its most general sense, risk can be defined as the combination of the probability of an event occurring and its consequences and constitutes both "opportunities" for benefit (upside) and "threats" to success (downside) [20], in the context of this work, only those undesirable events with negative consequences are considered and need to be mitigated.

One of the hurdles that prevent a Cloud service consumer from adopting Cloud services is the lack of adequate confidence of those services in term of the uncertainties associated with their qualities and levels in the ecosystem. Although the provision of a zero-risk service is not practical, if not impossible, an effective and efficient risk assessment of service provision, together with corresponding mitigation mechanisms, may at least provide a technological insurance that will lead to a higher confidence of Cloud service consumers on one side and a cost-effective and reliable productivity of Cloud Service Provider (SP) and resources organized by individual Infrastructure Provider (IP) on the other side. In this research, confidence is defined as the expectation of a successful fulfillment of a Service Level Agreement (SLA) agreed between a Cloud service consumer and an SP. The notion of "cost-effective and reliable productivity" is defined as a provider's capability of fulfilling an SLA through the entire cycle of the service provision, and at the same time realizing its own business level objects of an SP (e.g., make a certain amount of profits) and high resource utilization efficiency of an IP. By aiming this win-win target, this research work proposes a general risk assessment framework of Cloud service provision in term of assessing and improving the reliability and productivity of fulfilling an SLA in a Cloud. Based on this framework, a software toolkit is being designed and implemented, as a basic risk factor related optimization module, which is able to be integrated into other high level Cloud management and control software systems for both SP and IP.

Although risk factor related assessments for deciding risk levels are the main concerns of this work, we also consider that the decision making procedure of how to apply corresponding mitigation solutions to already identified risks in a Cloud Service Ecosystem may involve considerations on other higher level factors such eco-efficiency, cost, security and trust. In case such factors constrain the application of mitigation solutions in one way or another, certain mitigation strategies should be identified to optimize the executions of these mitigation solutions.

 ISBN: 978-1-61208-153-3

The main objective of OPTIMIS (Optimized Infrastructure Services) project [6] is to enable an open and dependable Cloud Service Ecosystem that delivers IT services that are adaptable, reliable, auditable and sustainable both ecologically and economically. The key goal of OPTIMIS is to allow organizations to automatically and seamlessly externalize services and applications to trustworthy and auditable Cloud providers. In the context of OPTIMIS, risk assessment will be applied at the Cloud service construction, deployment and operation phases supporting a wide range of scenarios such as Cloud bursting and Cloud brokerage that will be present in a fully developed Cloud Service Ecosystem of the future. Such mechanisms for managing risk for Cloud-based services which consider inherent aspects of Clouds such as energy consumption, the cost of reconfiguration and migration, and the reliability and dependability of the provided services will maintain secure, cost-effective and energy-efficient operations.

The main contributions of this paper are the design and implementation of an effective and efficient risk assessment framework (methodologies of risk identification, evaluation, mitigation and monitoring) for Cloud service provision. Together with the corresponding mitigation strategies, the framework provides technological assurance that will lead to higher confidence in Cloud providers for Cloud service consumers on one side and cost-effective, reliable and productive Cloud service provider's resources on the other side.

The rest of the paper is structured as follows: in Section II, related work on applying risk management methodologies into utility computing areas, such as Grids and Clouds is surveyed. The risk assessment framework for Cloud Service Ecosystems proposed by this research work is described in Section III; the corresponding software toolkit for the implementation of this risk assessment framework is discussed and introduced in Section IV; in Section V, use cases of the framework and software toolkit in the context of the OPTIMIS project are introduced. Finally, the conclusion of current work in progress is presented in Section VI, in which future work is also introduced and discussed.

II. RELATED WORK

In recent years, the principles and practices of risk assessment/management were being introduced into the world of utility computing such as Grid and Clouds either as a general a methodology [5][7]14] or focusing on a specific type of risk, such as security and SLA fulfilment [13] and [19]. In this section, we conduct a balanced introduction to cover these two aspects.

In [1], an extended Confidentiality Risk Assessment and Comparison (CRAC) method [2], CRAC++, is proposed to assess confidentiality risk in IT outsourcing. The aim of this method is to enable the specification of confidentiality requirements in an SLA between a client and IT resource provider. The method claims that it is able to satisfy six criteria of confidentiality level specification approach: specified confidentiality level is not based on percentages of data loss; assessment is not based on monitoring incidents, no disclosure of confidential information is required to a provider, ease of use; it is repeatable and will increase the client's understanding of confidentiality risks in this outsourcing relationship. The most unique feature of the method is that it tackles two hard problems regarding the specification of confidentiality requirements: 1) confidentiality incidents cannot be monitored, since attackers who breach confidentiality try to do this unobserved by both client and provider, and 2) providers usually do not want to reveal their own infrastructure to the client for monitoring or risk assessment.

In [3], the design, implementation and evaluation of separate and integrated risk analysis methods for a commercial computing service to support successful utility computing model is introduced. By departing from two new challenges facing a commercial computing service in order to support a utility computing model: (i) "what are the objectives or goals it needs to achieve in order to support the utility computing model", and (ii) "how to evaluate whether these objectives are achieved or not", the paper identifies four essential objectives that are required to support the utility computing model: (i) manage wait time for SLA acceptance, (ii) meet SLA requests, (iii) ensure reliability of accepted SLA, and (iv) attain profitability. Based on the analysis on the nature of these objectives, "risk assessment on resource management policy" is identified as the key evaluation methodology to examine whether resource management policies are able to achieve the objectives. Both the separate and integrated risk analysis methods evaluate a policy using two indicators: performance, as the value measure of the policy, and volatility, as the risk measure, that is able to "reflect how performance values fluctuate and thus the consistency of the policy in returning similar performance values". The separate risk analysis analyses the performance and volatility involved in a single objective for a particular scenario and the integrated risk analysis assesses a combination of multiple objectives with different weights used to denote the importance of each objective. These weights for various objectives provide a flexible means for the service provider to easily adjust the importance of an objective and determine its level of impact on the overall achievement of a combination of objectives. Most importantly, the crucial impact of the integrated risk analysis method is emphasised by simulation results that "an objective that is not achieved can severely impact on the overall achievement of other objectives. Thus, it is essential to examine the achievement of all key objectives together, rather than each standalone objective to correctly identify the best policy that can meet all the objectives."

In [4], a novel "insurance" mechanism is proposed as a risk management method that is "primarily used to hedge against the risk of a contingent loss due to unfavourable and uncontrollable events". According to this mechanism, a service insurer in the Cloud is established to decide and collect insurance premium from a service provider, send

 ISBN: 978-1-61208-153-3

compensation to a service consumer; a service provider negotiates an insurance contract with the service insurer; a service consumer submits a claim to the service insurer. Since a service consumer is not the payer of premium but able to claim compensation in case a loss was caused by the service provider, it will be relatively "risk free" for the consumer to use the service confidently. A Cloud Risk Assessment and Management (Insurance) Reference Model, is established based on the extended Zachman framework [9] with the service/information assurance, integrity and analysis, and also the layered reference Service Oriented Architecture (SOA) security reference model [10].

In [13], a quantitative risk and impact assessment framework (QUIRC) is presented to assess the security risks associated six key categories of security objectives (SO) (i.e., confidentiality, integrity, auditability, multi- party trust, mutual auditability and usability) in a Cloud computing platform. The quantitative definition of risk is proposed as a product of the probability of a security compromise, i.e., an occurring threat event, and its potential impact or consequence. The overall platform security risk for the given application under a given SO category would be the average over the cumulative, weighted sum of *n* threats which map to that SO category. In addition, a weight that represents the relative importance of a given SO to a particular organization and/or business vertical is also necessary and their sum always adds up to 1. This framework adopts a wide-band Delphi method [18], using rankings based on expert opinion about the likelihood and consequence of threats, as a scientific means to collect the information necessary for assessing security risks. The advantage of this quantitative approach of risk assessment is that it enables vendors, customers and regulation agencies the ability to comparatively assess the relative robustness of different Cloud vendor offerings and approaches in a defensible manner. However, the challenge and difficulty of applying this approach is the meticulous collection of historical data for threat events probability calculation, which requires data input from those to be assessed Cloud computing platforms and their vendors.

In [5], a SEmi-quantitative BLO-driven Cloud Risk Assessment (SEBCRA) approach that is aware of the Business-Level Objectives (BLOs) of a given Cloud organization is presented. The approach is designed for a Cloud Service Provider (CSP) to improve the achievement of a BLO, i.e., profit maximization, by managing, assessing, and treating Cloud risks. The core concept on which this approach is based is that "Risk Level Estimation for each BLO is proportional to the probability of a given risk and its impact on the BLO in question". Once risk has been assessed, the Risk Treatment sub-process defines potential risk-aware actions, controls, and policies to conduct an appropriate risk mitigation strategies, such as, avoid the risk, by eliminating its cause(s), reduce the risk by taking steps to cut down its probability, its impact, or both, accept the risk and its related consequences or transfer or delegate the risk to external organizations. In an exemplary experimentation, the risk assessment approach demonstrates that it enables a CSP to maximize its profit by transferring risks of provisioning its private Cloud to third-party providers of Cloud infrastructures. This risk assessment approach can be extended to tackle scenarios where multiple BLOs are defined by a CSP and also work as an autonomic risk-aware scheduler, which will be based on business-driven policies and heuristics that help the CSP to improve its reliability.

The work in this paper focuses on a framework that supports risk assessment at the Cloud service deployment and operation phases. It supports not only service and infrastructure providers, but a wide range of scenarios such as Cloud bursting and Cloud brokerage as well.

III. A RISK ASSESSMENT FRAMEWORK

Risk assessment allows improving the foundations of the Cloud infrastructure to help manage and anticipate the risks or opportunities:

- Helping to provide a framework for identifying the risks that present threats to the Cloud.
- Facilitating discussion among the various partners during the development process.
- Foresee potential dangers or risks before they occur and implement mitigation strategies to compensate for them.
- Building an infrastructure for monitoring these risks over time and identifying new risks when they arise.

In Cloud computing, risk needs to be considered at all phases of interactions and investigated at each service stage in relation to the *assets* which need to be protected. Two stakeholders are involved: Service Providers (SP) during the service deployment and operation, and the Infrastructure Providers (IP) during admission control and internal operations. In OPTIMIS, various use cases will be considered for depicting a Cloud scenario as discussed in Section V. These use cases will affect the assets involved as well as the kind of interactions taking place presenting new challenges for risk assessment.

In addition to the different use cases and interactions, risk will be assessed based on *categories* which will help to manage it and the mitigation strategies to be applied. For instance all risks associated with service level agreements (SLAs) can be identified as legal issues and would thus need mitigation strategies from the legal realm.

In addition to identifying the risk categories, each risk item will be assessed thanks to a level of impact and likelihood. For simplicity, the risk level can be labeled in the range from 1 to 5 to show its intensity (1-very low, 2- low, 3-medium, 4- high, 5-very high). The risk level will help manage the risk items from most threatening to the least impact helping with the mitigation strategies to be adopted later. This information will be available in the risk inventory.

A. Service Provider

A service provider is responsible for matching the end-user requirements with the correct IPs to ensure the required demand is met. To achieve this, the SP needs to be risk aware of each IP and ranks them accordingly.

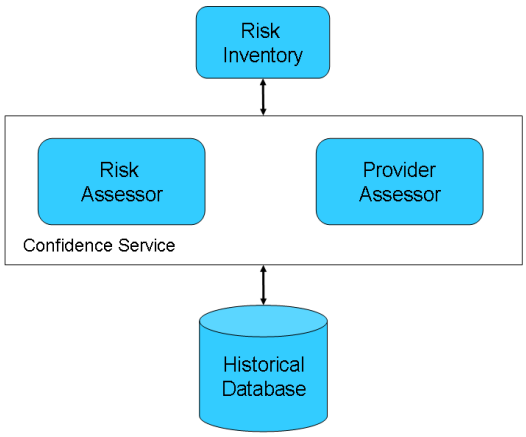

Figure 1. Service Provider – Risk Assessment Components.

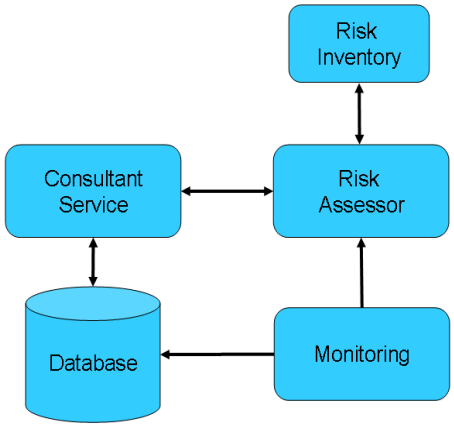

Figure 2. Infrastructure Provider – Risk Assessment Components.

Figure 1 shows the various components the SP will use to fulfill its purpose - a Confidence Service (comprising a Risk Assessor and a provider assessor), a risk inventory and a Historical Database for recording past SLA transactions. The confidence service will take into account the various risks of working with the different IPs accessing the providers. This will be part of the Service Deployment Optimizer (SDO). The SDO will make these decisions based on a stored database of history of working with the different IPs and the risk inventory associated with the different assets involved. A risk inventory is a simple database of risks associated with each asset, their vulnerabilities and threats. This would also contain risk mitigation strategies following risk assessment. All these factors will be accessed by the SDO to choose an efficient selection of the infrastructure provider to run the deployed service.

B. *Infrastructure Provider*

Performing risk assessment at this level increases the performance and quality of the IP. When the SP assesses the IP, the IP would also be assessing the service to be deployed. It will determine an estimated risk if it were to accept the SLA taking into account fault tolerance mechanisms and actions following an SLA violation, in turn improving the IP's reliability and quality of service.

The SP would send a service *manifest* request to the IP containing the feasibility of admitting the new service, with respect to current infrastructure load, predicted future capacity, as well as risk. This helps the IP to determine where to place the virtual machines (VMs) by combining its local management policy with the functional and non-functional requirements.

Figure 2 depicts the structure of the IP risk assessment components. The consultant service takes into account the risk assessor and the database to estimate the risk. This may use data mining tools on the previous history of events of running similar services or working with the same SP. The consultant service can also have access to all the monitoring information keeping the IP on track with the changes. This data can be static or dynamic in nature about its resources and the current service execution.

Examples of such information are the current workload, system outages, temporary performance shortages, monitored network traffic, experts' availability, or general information regarding the number of services to operate. The monitored data helps to determine bottlenecks in the IP's infrastructure so that the provider can improve its capacity planning, administration, and management of its resources. This leads to higher, cost-effective productivity of virtualized resources [21][22].

C. *Risk Inventory*

Various research areas such as business have developed risk inventories for determining how certain risks can be managed and evaluated to be brought up to an acceptable level. Most of the steps towards creating and refining of a risk inventory differ in relation to their purpose and context in which they are applied. A set of processes are identified to create and manage a risk inventory for the implementation of the framework:

1. Determine which use case scenario to focus on.
2. Determine the areas of interaction in the Cloud. Interaction takes place at various levels such as end-user to service provider or service provider to infrastructure provider. During each of these levels an SLA is agreed between parties and its fulfillment monitored.
3. Identify the assets involved which need to be protected from external or internal dangers (risk), as well as the vulnerabilities and threats these assets may have during operation.
4. Identify the risk triggering factors for these assets.
5. Identify the relationships between assets and various factors or events which may lead to risk mitigation.

Therefore the risk mitigation strategy would depend on the use case, asset at risk, and the event which may lead to activate the risk mitigation strategy to reduce it. Risk may also be dynamic and change depending on the situation and activities in the Cloud. These could be changes in policies, transactions etc. This introduces an additional dimension to the risk mitigation strategies which may vary with time.

 ISBN: 978-1-61208-153-3

D. Risk Assessment Models and Risk Categories

Risk assessment also depends on the time of operation during the Cloud service lifecycle. This allows the risk level to change over time. Various risk models can then be introduced to choose relevant mitigation strategies related to concrete situations and recognized threats. The risk models being investigated for this purpose are as follows:

- Probabilistic Risk Model - Risk is a compound of the probability of a problem occurring and the impact of the problem occurring. The probability would depend on the frequency of past problems over time.
- Possibilistic Risk Model – using stochastic processes such as Gamma distributions to predict the failure of a physical machine, Virtual Machine (VM) etc.
- Hybrid Risk Model – A combination of the two above models to predict and assess the risk on the probability of occurring events. Hybrid risk models allow different kinds of risks to be measured. This is because certain aspects can have a numerical probability attached to it for the risk actually occurring, but some events may have a dynamic nature to them, as certain exposures may lead to various relationships among the variables to actually propagate the risk.

Such models have been the focus of the work in [19] to enable a Grid provider to identify infrastructure bottlenecks (considering physical machines only) and mitigate potential risk, in some cases by identifying fault-tolerance mechanisms to prevent SLA violations. Moreover, a Grid broker provides the functionality to evaluate the risk associated with such provider by incorporating provider reliability into the risk models in order to verify the expected integrity of a provider's guarantees when they make any SLA offer [23].

Risk Category: **Technical**
Asset identified: Hardware
Vulnerability of asset: Poor maintenance
Threat to asset: Unresponsive system
Resulting risk item: Reduction in availability
Risk Likelihood: Low (2) [Range 1-5]
Risk Impact: Medium (3) [Range 1-5]
Resulting Risk level: Product of risk likelihood and risk impact [Range 1-25]
Risk event: Hardware failure
Resulting risk mitigation: Duplicate data, maintain hardware

Risk Category: **Policy**
Asset identified: SLA
Vulnerability of asset: Lack of jurisdiction information
Threat to asset: Breach in data confidentiality
Resulting risk item: Changes in jurisdiction
Risk Likelihood: Very high (5) [Range 1-5]
Risk Impact: High (4) [Range 1-5]
Resulting Risk level: Product of risk likelihood and risk impact [Range 1-25]
Risk event: Redeployment of data
Resulting risk mitigation: Seek legal advice

Risk Category: **General**
Asset identified: Security
Vulnerability of asset: Unprotected password
Threat to asset: Unrestricted access to data
Resulting risk item: Data leaks
Risk Likelihood: High (4) [Range 1-5]
Risk Impact: High (4) [Range 1-5]
Resulting Risk level: Product of risk likelihood and risk impact [Range 1-25]
Risk event: System hacks
Resulting risk mitigation: Encrypting data

Risk Category: **Legal**
Asset identified: SLA
Vulnerability of asset: Illegal clauses in the contract
Threat to asset: Sued
Resulting risk item: Ongoing legal dispute
Risk Likelihood: Low (2) [Range 1-5]
Risk Impact: High (4) [Range 1-5]
Resulting Risk level: Product of risk likelihood and risk impact [Range 1-25]
Risk event: Negligence
Resulting risk mitigation: Audit SLAs

Figure 3. Examples of Risk Categories.

The risk models under investigation will be applied to assess the risk on a number of groups of risks or categories. The various risk categories identified, with an example of an associated risk are:

- *Technical* – Hardware, VM failure
- *Policy* – Data jurisdiction policies or other issues which match requirements and considerations (prior to deployment).
- *General* – Various general issues such as security, data applications or processes (as assets to be protected during the different phases of the cloud lifecycle).
- *Legal* – SLA issues

An example of each of category is presented in Figure 3.

E. Risk Mitigation Strategies

Following the assessments on various risk factors and identification of associated mitigation solutions, where possible, appropriate mitigation strategies will be decided to implement these solutions. In general, mitigation strategy can be risk avoidance, limitation, retention**,** transfer and acceptance [11]. Within the context of our work, risk avoidance and limitation are the main strategies to be applied and the selection and execution of mitigation solutions will be considered as an optimization problem.

Since the nature of mitigation is to take precautionary actions before the occurrence of risk, time constraint and cost of a mitigation solution are key factors for deciding which mitigation strategies to choose and how to deploy them. When multiple risk factors need to be mitigated at the same time, it will be more complex to make an optimized decision under time and cost constraints. One example is that a set of

 ISBN: 978-1-61208-153-3

risk mitigation tasks with known, arbitrary execution times, need to be implemented by some identical high level risk mitigation solution executers by a given deadline. The problem is to schedule all of the mitigation tasks onto the least number of executers so that the deadline is met. This is a classic One-Dimensional Bin Packing problem in particular and combinatory optimization problem in general. Hence, this work is investigating optimization algorithms to help make decisions for scenarios as illustrated in these examples.

IV. A RISK ASSESSMENT SOFTWARE TOOLKIT

One of key design principles of a risk assessment software toolkit is to make it a self-contained independent functional component that is able to perform for Infrastructure Providers (IPs) and Service Providers (SPs) and be adopted, in either full or in part, by higher level Cloud management and control software system for higher level optimization purposes such as SP's brokerage for multiple IPs.

Following the logical structure of the risk assessment framework described in Section III, the toolkit is designed to physically consist of two independent parts: SP Risk Assessment Tool (SPRAT) and IP Risk Assessment Tool (IPRAT). For the SPRAT, its high level functions (e.g., evaluate the reliability of a specific IP offer) are mainly exposed by its external interfaces defined in its Confidence Service sub-component. Other lower–level functions such as the evaluation of the risk associated with an IP's offer and evaluation of IP's profile is provided by the external interfaces of the Risk Assessor sub-component and the Provider Assessor sub-component respectively. The Risk Inventory and Historical Database sub-components are private to the SPRAT and no external interfaces are provided by them. The Risk Inventory is designed as a knowledge base to consist of facts, scenarios, and reasoning rules for risk assessments related decision-making activities of the SPRAT.

For the IPRAT, its high level functions (e.g., evaluate the risk fulfilling a given service manifest of a specific SLA) are mainly exposed by its external interfaces defined in its Risk Assessor sub-component. Other lower–level functions such as data-mining of past failure events in an IP are provided by the Consultant Service sub-component. These lower-level functions are not purely private for the IPRAT. The Risk Inventory and Historical Database sub-components are also private to the IPRAT and no external interfaces are provided by them. For the IPRAT, its Risk Inventory is designed as a knowledge base to consist of facts, scenarios, and reasoning rules that are related to lower level hardware and software resources. The Historical Database sub-components is also private to the IPRAT. In addition, IPRAT's Monitoring sub-component includes two parts: one is the risk event detection and alarm part, and the other one is the lower-level hardware and software runtime status collectors. From the implementation perspective, the second part can be based on a third-party data monitoring and collection software, such as Nagios [12], as a plug-in, and will depend on the scalability and efficiency of it.

V. USE CASES IN THE CONTEXT OF OPTIMIS

In the OPTIMIS toolkit, risk is analyzed in the context of three dimensions: use case, actor and time. The toolkit tackles five Cloud uses cases that are in various stages of realization in the current Cloud ecosystem. They are: i) Private, ii) Bursting, iii) Multi-Cloud, iv) Federated and v) Brokerage [6]. These use cases have various implications for OPTIMIS as the differing goal of each contribute to what vulnerabilities an asset may have and thus its associated risk factors. The different Business Level Objectives of the SP and IP actors play a part in deciding the importance of risk because the execution of high-level strategies alter the importance and applicability of risk in a given situation. In addition, the lifecycle of a Cloud service adds a temporal aspect to risk assessment. Cloud Service Lifecycle is comprised of three phases: Service Construction, Service Deployment and Service Operation.

At Service Construction a service is developed, composed and configured. This entails packaging the core elements of a service and its dependencies together, the configuration of the service manifest that describes the functional parameters of each core element within the service and preparation of the VM images used to run the service. The Service Deployment phase sees the deployment of a service onto an IP. An IP is selected using a filter mechanism to decide, using Trust, Risk, Eco-efficiency and Cost (TREC) factors, which IP is most suitable to use for a given service manifest.

Finally at Service Operation, a service begins execution on a selected IP and is continually monitored.

A. Optimis Cloud Use Cases

The use cases are outlined in the following subsections and illustrated in Figure 4 which provides the vision of the OPTIMIS Cloud ecosystem.

1) Private Cloud

In the Private Cloud use case an SP and IP within the same administrative domain cooperate to provision resources for one or more services using internal infrastructure.

2) Cloud Bursting

In the Cloud Bursting use case an IP at some point during the operation of a service may require additional capacity to manage increases in demand above that which its local infrastructure can accommodate. This requires an IP to initiate the SLA negotiation process with another IP.

3) Multi-Cloud

The Multi-Cloud use case is an extension of the Cloud Bursting use case where by an IP may make use of multiple IPs to provision additional resources. The use case can be distinguished from bursting in regards to the IP selection mechanism used, which evaluates the functional and non-functional requirements of the service manifest and chooses the most appropriate IP for a given component of a service.

4) Federated Cloud

 ISBN: 978-1-61208-153-3

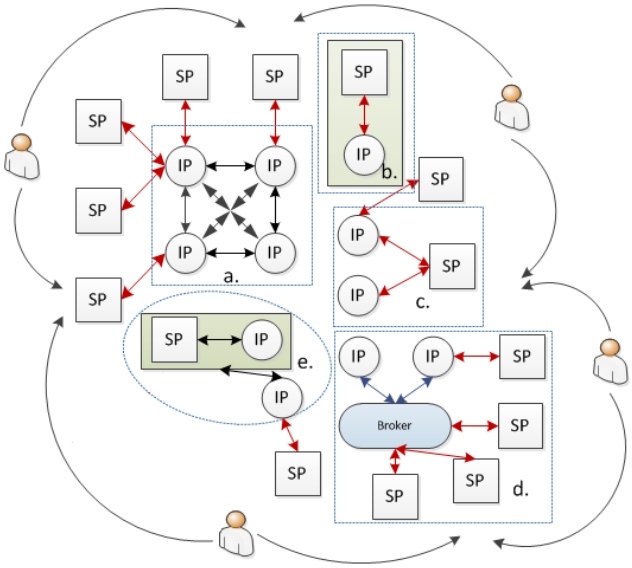

Figure 4: Interactions between Actors on a per Use Case Basis: (a) Federation, (b) Private, (c) Multi-Cloud, (d) Brokerage, and (e) Bursting.

In the Federated Cloud use case an IP provides resources for an SP on behalf and across a collective of IPs working in collaboration. This use case differs from the Multi-Cloud use case as the IPs have previously entered into a mutual SLA between all members of the federation before coming into contact with the SP.

5) Cloud Brokerage

The Cloud Brokerage use case sees the addition of a third actor into the Cloud ecosystem the Broker. The broker acts as an intermediary that facilitates the Cloud Lifecycle and adds value through maintaining a historic database of its encounters with SPs and IPs providing a mechanism to gauge the past performance of an actor and its ability to adhere to SLAs.

B. Stages of Risk Assessment in the Use Cases

Taking into consideration the Cloud Service Lifecycle in the context of the Risk Assessment Tools, assessment will be performed at many stages and will be reliant on the specific use case. Figure 5 depicts the general view of risk assessment in all the different use cases in OPTIMIS. The risk assessment stages will be dependent on the use cases being represented. The different use cases will influence the different actors allowing similar risk assessment between them. In the case of the private cloud, the actors involved were the Service Provider and the Infrastructure Provider (as shown in Figure 5). In the cases of Cloud bursting, federated and multi-Cloud, this will allow further actors to be involved depicting infrastructure provider and infrastructure provider interactions.

There are six action stages which are dependent on the interaction of an SP and IP and what tasks it is performing and will dictate what risk models and input data are utilized in the assessment.

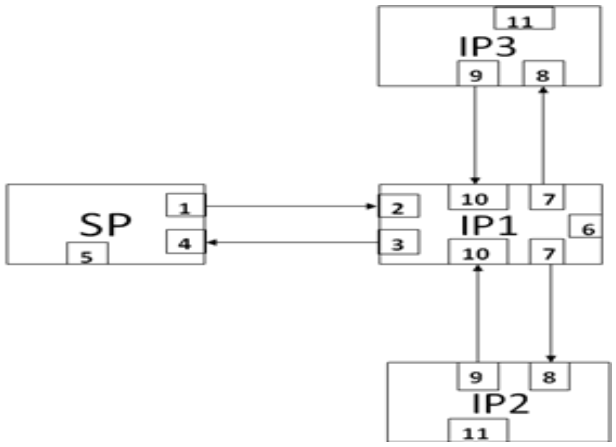

Figure 5: Risk Assessment Steps 1-11 in the Different Use Cases.

The six action stages are as follows:

- Action 1: The sender, before sending an SLA request to an IP, assesses the risk of dealing with all known IPs.
- Action 2: An IP receives an SLA request and assesses the risk of dealing with the SP from which the request came from.
- Action 3: The IP assesses the risk of the SLA from the sender and evaluates the risk associated with the service manifest.
- Action 4: The sender then receives the IPs SLA offer and assesses the risk associated against other IP SLA offers.
- Action 5: The sender performs continual risk assessment at Service Operation, monitoring service level non-functional QoS metrics such as response time.
- Action 6: The receivers perform continual risk assessment at Service Operation, monitoring low level events from the infrastructure such as risk of VM failure.

For the private cloud the 6 stages in Figure 5 will be from steps 1-6 in which each of the 6 actions take place. The order in which each of the action stages is (Step 1-Action 1), (Step 2 -Action 2), (Step 3-Action 3), (Step 4-Action 4), (Step 5-Action 5) and (Step 6-Action 6).

In Cloud Bursting use case four further stages of risk assessment occur between the IP1 and IP2 that replicate the risk assessment performed by the SP in the Private Cloud use case, where by IP1 takes on the negotiation roles of the SP to facilitate the acquisition of additional resources. The additional number of action stages is (Step 7-Action 1), (Step 8 -Action 2), (Step 9-Action 3), (Step 10-Action 4), (Step 11-Action 6).

In the Federated Cloud use case, due to the collaborative nature of the IPs and the assumed prior SLA between the members of the federation, this use case is a simplification of Cloud Bursting with the exception that any number of IPs

 ISBN: 978-1-61208-153-3

can be burst to and a single IP resumes the role of being the point of entry into and controller of the federations. This means no risk assessment is necessary in regards to risk assessment steps 7 to 10 of the Cloud Bursting use case. Therefore there are only Steps 1-6 with an additional Step 11.

Finally, in the Multi-Cloud use case the missing steps of risk assessment in the Federated Cloud use case are necessary as IP1 is required to select and negotiate with several IPs. Therefore it will use all the steps from Step 1-11 for its risk assessment in multi-cloud scenario.

VI. CONCLUSION AND FUTURE WORK

This paper presents various methodologies being designed and developed for performing risk assessment on both SP and IP levels. The main contributions of the work are the design and implementation of an effective and efficient risk assessment framework (methodologies of risk identification, evaluation, mitigation and monitoring) for Cloud service provision. Four risk categories, namely legal, technical, policy, and general have already been identified. SP and IP risk models are being investigated in conjunction with a risk inventory for Cloud computing specific to OPTIMIS through various use cases: private cloud, cloud bursting, multi-clouds, federated cloud, and cloud brokerage. This inventory is populated with Assets, Incidents/Risk Scenarios and Impact/Consequences, as well as associated mitigation strategies. The novel risk assessment models will be built and developed as a combination of probabilistic, possibilistic and hybrid models to suit each risk category identified in the risk inventory.

ACKNOWLEDGMENT

This work has been partially supported by the EU within the 7th Framework Programme under contract ICT-257115 - Optimized Infrastructure Services (OPTIMIS).

REFERENCES

[1] A. Morali and R. J. Wieringa, Risk-Based Confidentiality Requirements Specification for Outsourced IT Systems, pp. 199-208, Proceedings of the 18th IEEE International Requirements Engineering Conference, 2010, DOI 10.1109/RE.2010.30.

[2] A. Morali and R. J. Wieringa, Risk-Based Confidentiality Requirements Specification for Outsourced IT Systems (ex-tended version), Technical Report TR-CTIT-10-09, Centre for Telematics and Information Technology, University of Twente, 2010.

[3] C. S. Yeo and R. Buyya, Integrated Risk Analysis for a Commercial Computing Service in Utility Computing, Journal of Grid Computing, Volume 7, Number 1, pp. 1-24, ISSN: 1570-7873, Springer, Germany, March 2009.

[4] M. Luo, L. J. Zhang, and F. Lei, An Insurance Model for Guaranteeing Service Assurance, Integrity and QoS in Cloud Computing, pp. 584-591, Proceedings of the 2010 IEEE International Conference on Web Services, DOI 10.1109/ICWS.2010.113.

[5] J. O. Fitó, M. Maćas, and J. Guitart, Towards Business-driven Risk Management for Cloud Computing, pp. 238-241, Proceedings of the 2010 International Conference on Network and Service Management – CNSM 2010.

[6] A. J. Ferrer, F. Hernandez, J. Tordsson, E. Elmroth, C. Zsigri, R. Sirvent, J. Guitart, R. M. Badia, K. Djemame, W. Ziegler, T. Dimitrakos, S. K. Nair, G. Kousiouris, K. Konstanteli, T. Varvarigou, B. Hudzia, A. Kipp, S. Wesner, M. Corrales, N. Forgo, T. Sharif, and C. Sheridan, OPTIMIS: a Holistic Approach to Cloud Service Provisioning, in the Proceedings of the 1st International Conference on Utility and Cloud Computing (UCC 2010), Chennai, India, December 2010.

[7] K. Djemame, I. Gourlay, J. Padgett, K. Voss, and O. Kao, Risk Management in Grids, In R. Buyya and K. Bubendorfer, editors, Market-Oriented Grid and Utility Computing, pp. 335–353. Wiley, 2009.

[8] R. Alsoghayer and K. Djemame, Probabilistic Risk Assessment for Resource Provision in Grids, pp. 99-110, in the Proceedings of the 25th UK Performance Engineering Workshop, Leeds, UK, July 2009.

[9] J. A. Zachman, "A Framework for Information Systems Architecture", IBM SYSTEMS JOURNAL, VOL 26. NO 3, 1987.

[10] J. Heaney, D. Hybertson, A. Reedy, S. Chapin, T. Bollinger, D. Williams, and M. Kirwan, Jr. Information Assurance for Enterprise Engineering, in Proceedings of PLoP, Monticello, Illinois, 8-12 September 2002.

[11] G. Stoneburner, A. Goguen, and A. Feringa, Risk Management guide for Information Technology Systems, NIST Special Publication 8-00-30

[12] Nagios <http://www.nagios.org> 30.06.2011

[13] P. Saripalli and B. Walters, QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security , pp. 280-288, In the Proceedings of the IEEE 3rd International Conference on Cloud Computing, 2010

[14] X. Zhang, N. Wuwong., H. Li, and X. J. Zhang, Information Security Risk Management Framework for the Cloud Computing Environments, pp. 1328-1334, in the Proceedings of the 10th IEEE International Conference on Computer and Information Technology, 2010 (CIT 2010)

[15] IDC Cloud Computing Survey <http://blogs.idc.com/ie/?p=210> 30.06.2011

[16] ENSIA Report on Cloud Computing Security Risk Assessment <http://www.enisa.europa.eu/act/rm/files/deliverables/Cloud-computing-risk-assessment> 30.06.2011

[17] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, Above the Clouds: A Berkeley View of Cloud Computing, Technical Report. University of California at Berkeley, 2009.

[18] H. A. Linstone, The Delphi Method: Techniques and Applications. Addison-Wesley, 1975.

[19] K. Djemame, J. Padgett, I. Gourlay, and D. Armstrong, Brokering of Risk-Aware Service Level Agreements in Grids, Concurrency and Computation: Practice and Experience, 2011.

[20] The Risk Management Standard, Institute of Risk Management, The Association of Insurance and Risk Managers, National Forum for Risk Management in the Public Sector, Volume 2008, 21st August, 2002.

[21] Optimis Consortium, Architecture Design, WP 1.1: Requirements Elicitation, 2010 <http://www.optimis-project.eu/publications> 30.06.2011.

[22] Optimis Consortium, Architecture Design, WP 1.2: Reference Architecture, 2010 <http://www.optimis-project.eu/publications> 30.06.2011.

[23] C. Carlsson, Risk Assessment for Grid Computing with Predictive Probabilities and Possibilistic Models, in proceedings of the 5th International Workshop on Preferences and Decisions, Trento, Italy, April, 2000.

 ISBN: 978-1-61208-153-3