The Estimation of Risk on Cloud Computing Framework

Rashmi Priya

Abstract: The Cloud Service which is provided generates access to the present resources by service level agreements (SLA) which is formal , and they require proper balanced infrastructures in order to maximize the quality of service (QoS). They try to minimize and provide offer to the count of violations that are offered by the Service Level Agreements. The paper emphasizes on a proper or area of risk assessment which is specific to the applications related to cloud computing. The methods which are present within a framework that is to be used by service providers related to cloud and consumers related service in order to provide assessment of risk in case of deployment of service and the related operation. The paper also puts emphasis on the different stages which are involved in the lifecycle of services where assessment of risk takes place. This leads in the design and implementation of risk models which are in correspondence. The risk puts an impact on the architectural components providing special emphasis on management which is holistic to provide support at operation of services has been described. The assessor which is related to risk has been proven to be effective by various evaluation provided through the experiments and its implementation which needs to be integrated in a toolkit environment provided by cloud computing.

Index Terms: Cloud Computing, assessment of risk, model of risk, quality of service.

I. INTRODUCTION

Recently a large number of interest in commercialization has led to the research advances in cloud computing. The infrastructure of cloud supports services and applications which are required for commercial services and applications. There is a need of proper development in the areas of dependability and risk before making a reality to the large spread adoption of commercial application. So there is a need of incorporation of Risk Management in the infrastructure of cloud to provide the service to be followed by the infrastructure of cloud.

The advantages of risk management related to cloud computing results a conceptual necessity in supporting multiple parties which are related in getting decisions which are informed on agreements that are contractual. The confidence related to service provided by cloud is inadequate due to the uncertainties which are associated with quality level that may avoid consumer of cloud service from adoption of cloud technologies.

There is no provision of a risk which can be null in a cloud service provider, so an efficient and effective assessment of risk in consumption and provision of service which can be combined with mechanisms to mitigate risks that may minimally suffice a insurance which are technical which may provide a high confidence lead to the consumers of cloud service, and also a reliable and cost effective productivity which are reliable to service providers of cloud.

An end-user can be considered as a service provider who participates from the large public moving towards the cloud for performing a work that consists of multiple services. The kind of task which is to be performed needs to get an indication from the end user and requirements needs to be associated in formal to satisfy service level agreement(SLA). The desired information is applicable to the requirement placed by the end user for indicating the requirements which are associated and for the task of approaching for a service related to cloud in public. The information is based on the end-user desire in order to meet access with providers of infra-structure which are providing these services so that the task can be completed.

The access to services and resources is offered by IPs by identifying SLAs in order to specify risk, price and penalty. The end-users and IPs must interact and that can have governance through contract for definitions of obligations related to IP. The IPs and end users needs to be governed by several contract for defining the various obligations related to IP. The payment is to be done by the end-user and some penalty is to be imposed in such cases where the obligations is not fulfilled by any of the event. The SLAs and its requirement has to undergo various interactions in order to increase momentum in the area related to cloud computing. Moreover, there is a need for proper balanced infrastructures provided by IPs so as to gain at optimum level for the service quality to be achieved and also for reducing the number of violation related to SLA. The various approach desired helps to increase the related benefit due to economy and may help to motivate end-users to outsource tasks related to IT. A trustworthiness of IP is a prerequisite which provides ability in order to provide delivery of SLA successfully.

The assessment of risk is taken care of in different phases of lifecycle of service providers related to the stakeholders. The end-users are present in deployment of operation and service and during control and admission of service as well as internal operations IPs are used.

The assessment of risk in deployment of service is considered in the context as follows :- 1)Determining the risk to be dealt before an SLA request is sent to IPs. 2) When SLA request is received from IP determining the risk associated with dealing with end-user which has initiated the request. 3)The IP performs the control of admission determining the risk provided by accepting the request by SLA. 4)When an offer of SLA is received by end-user determining the risk which is associated when a service is deployed in an IP. The assessment of risk selects the IP to allow it to choose for acceptance of SLA requests.

Revised Manuscript Received on January 07, 2020.
* Correspondence Author

Dr. Rashmi Priya, Assistant Professor, GD Goenka University, Gurgaon, India.

The informed decisions must be made by end-users for decisions related to awareness of risk on the quotes linked to SLA which is received by the IPs leading to decision which balances time, risk and cost and is acceptable.

The benefit is received when risk is evaluated following an SLA violation as it offers them in determining the implications to economy resulting in offer by SLA in particular. The assessment of risk plays a major role when the associated with an IP is taken into account.

The assessment of risk support the given points in service operation 1) the risk related to failure of SLA from the perspective of end-user.2) determining the risk which may lead to failure of SLA which are specific from perspective of IP . Continuous assessment of risk is performed by IPs for operation of services towards monitoring low level events related to infrastructure which leads to risk when failure of Virtual Machines or physical hosts occurs leading to risk of data management, legal and security.

Assessment of risk has been taken into computing of utility with clouds and grids as a method in general or for focusing a type of risk which is specific related to SLA FULFILMENT. The idea of the paper is to propose a assessment of risk for provision of service of cloud in relation to improving and assessing the productivity and reliability of fulfilment of SLA in environment which has relation attached to cloud.

As per the framework given a software tool is implemented and designed as a module related to assessment of risk which is to be combined with the cloud management which is at the upper level and systems control of software systems which hold validity both for end users and IPS. The paper deals with existing research on risk assessment in association with cloud computing. The feature of SLAs related to cloud and the workloads which are associated are separate from those in other programs and so it effects the prediction of event and risks associated with cloud computing.

The major framework of this paper are as follows:-

An assessment of risk for cloud computing.

Assessment of risk is supported by deployment of service and operation which hold benefit for both end users and infrastructure providers. A related model which is linked to providers of infrastructure has to provide assessment of operation at level providing service which can lead to the failure of risk of 1) VMs 2) SLAs 3) entire cloud infrastructure and 4) physical nodes.

II. RISK MANAGEMENT

The area of management of risk displays an additional role in different fields related to economics, systems analysis, statistics, biology and operation research . There is a possibility of a hazardous event to have a sustenance related to the achievement of objectives. A risk measurement is related to consequence and the related likelihood associated with an event [6]. A qualitative assessment of risk is considered in proportion to the losses which are expected that can be caused because of any event and due to the probability of occurrence of this event. This quantitative representation of the consequences of probability of product may prove to be hazardous. The following are the concepts for risk management : a) it is an explanation of value to be assigned to party and for the protection that is required by party. b) the incident that is not required for cases where it harms or decreases the value provided by an asset. An incident which is caused as a potential which is not required is considered as a threat and any kind of vulnerability is considered as a weakness, flaw or deficiency which needs to open up or has to be exploited by any kind of threat which harms or tries to reduce the value related to an asset. Finally the likelihood of risk is any kind of incident which is not wanted and provides its consequence for asset which is specific and the risk imposed is the level or value assigned to a risk that is derived from the consequence and its likelihood. An asset for example is a server and a threat may be a computer virus and vulnerability to it is a virus protection which has not been updated that might cause an incident which is not wanted for example any hacker which can get access to the server. The probability of virus in order to create an entry from the back door to the linked server may be medium and the integrity linked to the server in consequence of getting impact causing harm may be high. An issue which is fundamental related to characterization and in representation of risk in order to appropriately and properly carry out the task follows the following steps :- a) the events triggering the risk needs to be analyzed in order to break down the events and provide adequate formulation of the structure in accurate. b) the losses needs to be estimated in association with the event for realisation of cases.

The probabilities of the events or its possibilities can be forecasted by the use of assessments that are probabilistic with the aid of statistical methods or judgements which are subjective with reasoning in approximation. The assessment of possible risks and its identification, helps to reduce the negative effects produced by the risk in order to measure severity of loss which has potential as per the occurrence of its possibility. The risk assessment and its input may range from simple steps to measurable steps while trying quantification of the events which are very unlikely. It helps to assess or measure risk based on the results for developing strategies in order to manage the risk and provide a control to its implications. In order to manage a risk types the issues which are related to determining if an action or any set of actions which is required and then to find the strategy of actions which are optimal in dealing with the assigned risk. The associated actions for acceptance or absorbance of the consequences whether some or total for a particular task can be applied for a comprehensive strategy that consist of combination of following measures in appropriation. The risk assessment analysis which is in quantitative needs to be performed on associated risks in order to prioritize an estimate which is numerical that is comprised of the probability that a harm is defined which procures result when a particular event is in occurrence.

In case of quantitative risk assessment analysis (QRA) is performed based on the risks to be prioritized and numerical estimation is provided which is based on the probability on which a defined harm can produce result based on the occurrence of event of particular type.

Those effects which are based on the risks related to events can be represented with representation of five point rating scale a) Trivial b) minor() c) significant() d)major e) catastrophic.

The paper has a focus on specific area related to risk management and methods which is to be used by provider of cloud for the evaluation of risk

through different stages of service lifecycle i.e. a) construction b) deployment and c) operation which is applied to areas of cloud computing. In the area related to this the assets which are included are physical nodes, SLAs and virtual machines. A node which is physical has to be considered as an asset under which case a threat generated may prove to be a loss to the connectivity provided and may lead to a vulnerable fault in the hardware that can lead to the resource and its failure due to incidence which are not wanted.

AWARENESS OF RISK ON CLOUD COMPUTING – FRAMEWORK

The vision in overall which tries to embrace an extended approach to different utility of computation of model related to business which can fit in a business model which is open market as for example in order to access infrastructure which works as a service to be used in various sectors like automotive, finance and energy as the provision linked to a framework in order to allow individuals for negotiation and consumption of resources of cloud by using agreements which are service level.

3.1 Service Life Cycle and Risk Assessment

A situation can be considered for the service requirements related to SP where the IP makes an offer related to SP. The SP can either commit related to the SLA or it can reject it. The risk can be considered in various phases related to service lifecycle for various stakeholders. SP can be used for construction of service, operation and deployment. IP can be used during control and admission of services and operations which are internal . In such cases the IP allows to offer the uses related to resources as a service which can be used as on pay basis for potential of SPs and which can allow the use of SLAs in order to guide interaction which is required in between.

3.2 Deployment of Service

The overview related to SP and IP interactions can be provided by infrastructure related to deployment of services in case the negotiation by SLA is encountered. The SP has an objective to provide support to planning related to business and strategic. The protection of specific assets is taken care by SP.

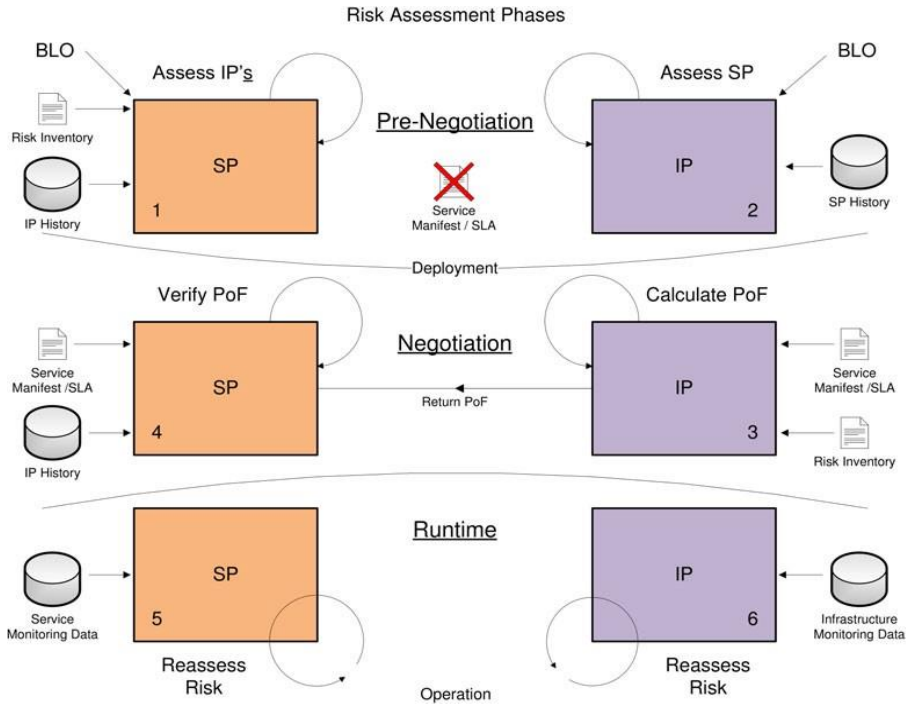


Fig. 1. Stages of Risk Assessment

The criteria for assessment are:

1. Geographical information. Geographic stability level, threat level, transparency of jurisdiction level, overlapping jurisdiction level.
2. Previous SLA performance. This includes the number of past successful SLAs.
3. Stability of Business. This for example includes the number of employees, and the number of customers business history,
4. Standards Compliance and Certifications . certification related to facility level, certification operation related level, and standard industry compliance level.
5. privacy general practice. data access and facility control level, data protection personal level.
6. infrastructure general practice. compute resources available, spare resources available, node availability average, backup storage frequency.
7. security general practice. security facility level.

Retrieval Number: D1188016420/2020©BEIESP
DOI: 10.35940/ijisme.D1188.016420

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

3.3 Summary

When a negotiation of SLA takes place the assessment of risk framework has been framed by allowing all the actors (SPs and IPs) can negotiate in order to consume cloud resources by using SLAs and moreover all the different risk models to be framed for which the actors required are to make use of various stages attached to the lifecycle of services.

While a service is under operation before commitment of an SLA, the risk of service unavailability is carried by SP by evaluation of reliability of IP in association with past behavior constantly monitored by SP to monitor execution of service and perform the assessment of risk on continuous basis to monitor the execution of service and perform assessment of risk on continuous basis as a part of fulfillment of SLA. Similarly the constant monitoring of infrastructure is done by IP for service operation and continuous performance of assessment of risk as a support of fulfillment of SLA.

III. MODEL

Risks individually associated with respect to each of the event (threat, vulnerability) needs to be first calculated and then an aggregation of risk in order to enhance knowledge which are based on the individual risks has been estimated. Within the assessment risk model, several elements in general which are related to risk has to be identified:

^{R}ji¼ ^{L}ji (1)

Risk related inventory: For this stage analysis and requirements is performed for identification of the inventory for which risk is populated.

Identification related to Vulnerability: A related vulnerability has to be considered as a flaw or weakness related to procedures of a design or internal, management controls system, that can be accidentally triggered or intentionally exploited. Let vulnerability of each type to be represented in terms of a single bit in the vulnerability vector:

V ¼ fV_i g ¼1 i 1, 2, . . . (2)

Where as Vi represents individual vulnerability. The value associated 1 indicates the present case of vulnerability in the system for assessment, else 0.

IV. IMPLEMENTATION

In order to optimize the whole service lifecycle it includes innovations OPTIMIS to be summarized with respect to a combination of technologies in order to create a dependable ecosystem related to cloud providers and consumers which will be the foundation of efficient operations related to services and various infrastructures.

Similarly SPs and IPs are decision making based not only on low-level functional properties, but additionally on non-functional factors which are related to risk (likelihood-consequence analysis for valuable assets),trust (including reputation), eco efficiency (power consumption and ecological factors), as well as cost (economical models for service and infrastructure provisioning expenses).

The OPTIMIS toolkit has to simplify for SPs and IPs for using OPTIMIS tools that can help in deciding whether to accept an additional services and also to optimize provisioning for the previously hosted ones.

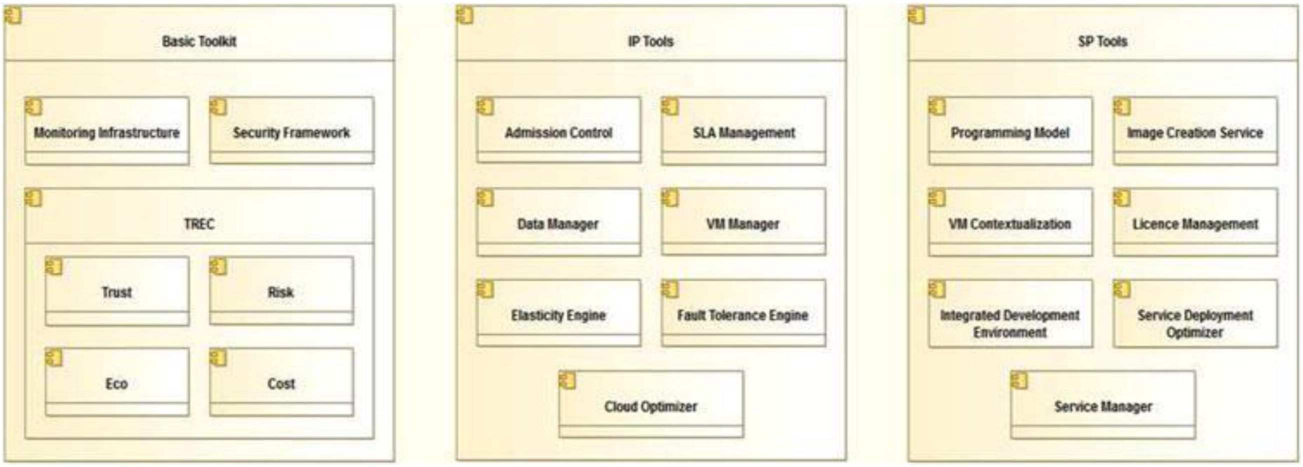


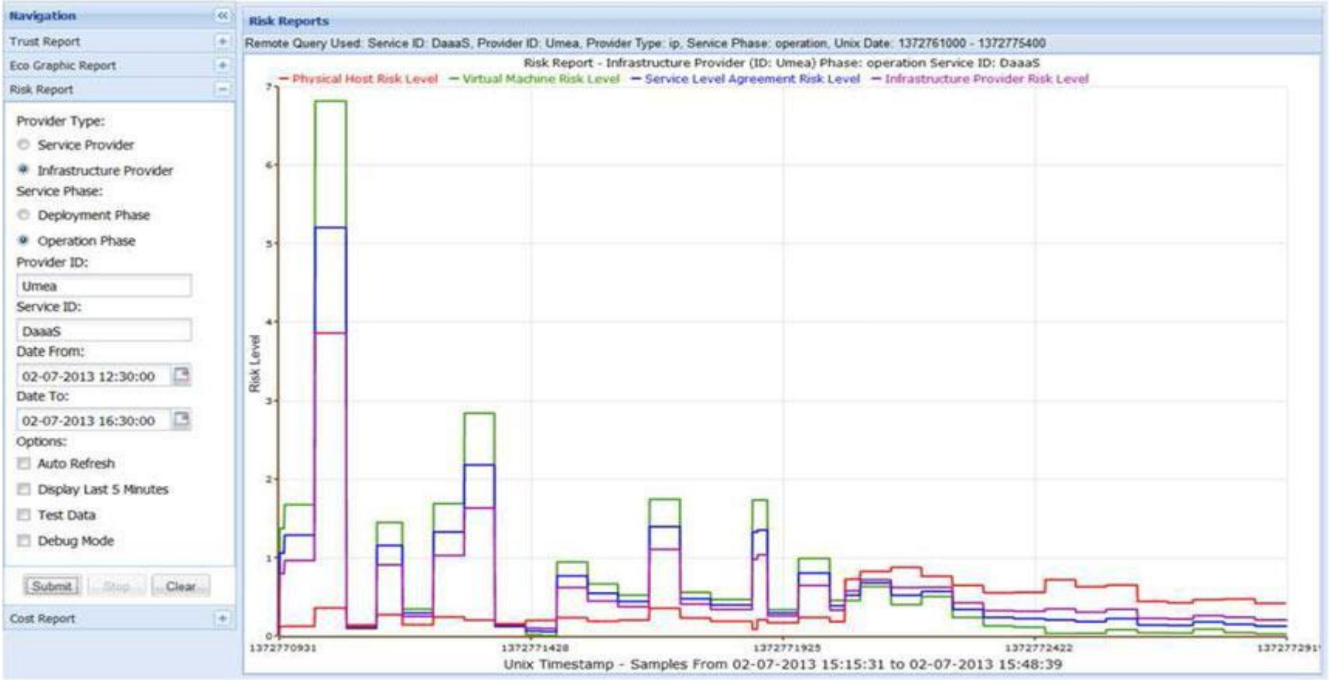
Fig.2. Overview of OPTIMIS toolkit.

V. EVALUATION

The experiment has been performed on the context of a system related to real cloud test bed by using the prototype which can help to evaluate the service operation of IP risk model, two experiments needs to be conducted as risk assessor. The second experiment is entitled to take a black box approach which fabricates input related to the risk assessor for enabling greater control on experimental variables.

This setting has been carried out by the HM on environment of cloud comprising of the following system a) two physical machines and b) Dual AMD Opteron 6234 (16 Core) Processors with 64 GB of RAM. The risk assessor needs to be deployed as a part of the wider OPTIMIS toolkit. An OPTIMIS manifest services to be deployed which comprises of VMs in total numbering eight and providing two virtual CPU cores and 2 GB of memory.

The IP risk assessment has to to fulfill high level BLOs which is directly linked service level goals which are in existence.


Navigation
Trust Report
Eco Graphic Report
Risk Report
Submit
Stop
Clear
Cost Report
Risk Reports
Risk Report - Infrastructure Provider (ID: Umea) Phase: operation Service ID: DaaaS
Physical Host Risk Level
Virtual Machine Risk Level
Service Level Agreement Risk Level
Infrastructure Provider Risk Level
Risk Level
0
1
2
3
4
5
6
7
1372770931
1372771428
1372771925
1372772422
1372772919
Unix Timestamp - Samples From 02-07-2013 15:15:31 to 02-07-2013 15:48:39

Provider Type:
○ Service Provider
● Infrastructure Provider
Service Phase:
○ Deployment Phase
● Operation Phase
Provider ID: Umea
Service ID: DaaaS
Date From: 02-07-2013 12:30:00
Date To: 02-07-2013 16:30:00
Options:
□ Auto Refresh
□ Display Last 5 Minutes
□ Test Data
□ Debug Mode

Remote Query Used: Service ID: DaaaS, Provider ID: Umea, Provider Type: ip, Service Phase: operation, Unix Date: 1372761000 - 1372775400

Fig. 4. Four levels risk assessment at service operation

6.1 Functional type Evaluation

The idea of this functional evaluation related to the risk assessor is to ascertain the experimental scenario which is to motivate via a hypothetical IPs that can help in maintaining profitability and can meet financial obligations to various stakeholders in order to effect the cloud environment and associated risk inventory by taking input on the output over time of the assessment model associated to risk for IP service operation by the use of fabricated metrics.

6.2 Experimental Setup

The evaluation has taken under consideration a hypothetical IP and the objective of this evaluation is entitled to expose the various relationship and correlation associated to the four risk levels linked to the model. Moreover, the experiment will show the effects of a various cloud environment associated to the risk models output and can disclose the ramifications related to running the assessments of risks on various types of service with different attributes that has ten physical machines with the listed characteristics: CPU Cores, 4 GB RAM, 1 Gbit NIC, 4 TB HDD, 0.001 per-cent probability of failure.

The first experiment has taken in consideration the impact of running 1 to 10 concurrent homogeneous services comprised of five VMs using a low variance workload. A new service is to be added every 10 time steps. This experiment has been repeated three times, each time using a different service profile. This experiment has to ascertain the impact of increasing resource utilization over time on the four risk levels. The second experiment has taken in consideration and two services using service profile and having low variance workload and service profile three with a high variance work load. Each service is composed of 10 VMs. This experiment will ascertain the impact of workload on risk level between concurrently executing services.

TABLE 1 Characteristics of Virtual Machine

Service Profile	CPU Cores	RAM	Network	Storage Of Disk	Chances Of Failure
1	1	512	100Mbit	100GB	0.00%
2	2	1024	100Mbit	200GB	0.00%
3	4	2048	100Mbit	300GB	0.00%

6.3 Results

The figure shows that as the capacity of the cloud increases the following section discuss the results of the three experiments using the previously outlined profiles and experimental setup show the results of running one to ten concurrent services using service profile one with five VMs per service.

This is highlighted in both the physical host risk level and the infrastructure provider risk level where physical resource capacity plays a larger role in these risk level calculation. As it would be expected, when many services with larger resource requirements are deployed in an infra-structure provider, the impact is seen more quickly across all risk levels. Additionally, these figures also illustrate that the risks associated with physical resource capacity do not have an impact on the risks associated with virtual resource capacity shows the relationship between the risk levels when the capacity of an IP is filled.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

VI. CONCLUSION

This paper has proposed scenarios which are motivating and needed for assessment of risk framework in area of cloud computing has been presented. The importance associated to risk assessment at different stages of the service life cycle has been identified, and the models associated for assessing the risk of pre-SLA negotiation, SLA negotiation, and service runtime are presented.

The model has acceptability on monitoring low-level events that the risk model linked to IP uses at various service operation in order to perform continual assessment of risk has been developed from various infrastructure in order to support the risk associated to failure. The relation to these four assets (physical hosts, VMs, SLAs, and IP infrastructure) considers vulnerabilities and threats which are associated with them. The software prototype has been accompanied with tool for visualization of the risk model has been implemented and then evaluated in the context of a cloud test bed of real type and through fabrication of monitoring of data in order to enable control over experimental variables that provides real-time feedback based on current service levels. It is combined in the risk assessment framework which is viable contender that can enable an IP in order to identify infrastructure and mitigate associated potential risks.

REFERENCES

1. J. O. Fito and J. Guitart, “Business-driven management of infrastructure-level risks in cloud providers,” Future Gener. Comput. Syst., vol. 32, pp. 41–53, Mar. 2014.
2. P. Saripalli and B. Walters, “QUIRC: A quantitative impact and risk assessment framework for cloud security,” in Proc. IEEE 3rd Int. Conf. Cloud Comput., 2010, pp. 280–288.
3. K. Djemame, J. Padgett, I. Gourlay, and D. Armstrong, “Brokering of risk-aware service level agreements in grids,” Concurrency Com- put.: Practice Exp., vol. 23, no. 7, pp. 1558–1552, 2011.
4. K. Misra, “ Risk analysis and management: An introduction,” in Handbook of Performability Engineering, K. Misra, Ed. London, U.K.: Springer, 2008, pp. 667–681.
5. (2013, Dec.). Iso 31000:2009 risk management-principles and guidelines [Online]. Available: http://www.iso.org/iso/catalogue_detail?csnumber=43170
6. W. Jansen and T. Grance, “Guidelines on security and privacy in public cloud computing,” Nat. Inst Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-144, 2011.
7. A. J. Ferrer, F. Hernandez, J. Tordsson, E. Elmroth, A. Ali-Eldin, C. Zsigri, R. Sirvent, J. Guitart, R. M. Badia, K. Djemame, W. Zie- gler, 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,” Future Gener. Comput. Syst., vol. 28, no. 1, pp. 66–77, 2012.
8. K. Djemame, I. Gourlay, J. Padgett, K. Voss, and O. Kao, “Risk management in grids,” in Market-Oriented Grid and Utility Computing. R. Buyya and K. Bubendorfer, Eds., Hoboken, NJ, USA: Wiley, 2009.
9. X. Zhang, N. Wuwong, H. Li, and X. Zhang, “Information security risk management framework for the cloud computing environments,” in Proc. 10th IEEE Int. Conf. Comput. Inf. Technol., 2010, pp. 1328–1334.
10. E. Network and I. S. Agency, “Cloud computing security risk assessment,” 2009.
11. Z. Hua, B. Gong, and X. Xu, “A DS-AHP approach for multi-attribute decision making problem with incomplete information,” J. Expert Syst. Appl., vol. 34, pp. 2221–2227, 2008.
12. K. Djemame, D. Armstrong, M. Kiran, and M. Jiang, “A risk assessment framework and software toolkit for cloud service ecosystems,” in Proc. 2nd Int. Conf. Cloud Comput., GRIDs, Virtualization, Rome, Italy, Sep. 2011, pp. 119–126.
13. K. Djemame and R. Alsoghayer, “Resource failures risk assessment modelling in distributed environments,” J. Syst. Softw., vol. 88, pp. 42–53, 2014.
14. A. Khan, M. Oriol, M. Kiran, M. Jiang, and K. Djemame, “Security risks and their management in cloud computing,” in Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci., 2012, pp.121–128.
15. M. Lund, B. Solhaug, and K. Stolen, Model-Driven Risk Analysis- The CORAS Approach. New York, NY, USA: Springer, 2011.