Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Importance of Risks Analysis with Monte Carlo in Cloud Computing

B Castro[1] And R Romero[2]
[1,2]*Departamento de Posgrado, Escuela Superior de Cómputo del Instituto Politécnico Nacional, Distrito Federal, México*

Abstract—Cloud computing promises to any company using information technology high availability, flexibility, increase efficiency, save money, etc .; but it raises questions about how best to protect your information and ensure compliance with the rules, considering a scenario of risk are involved where confidentiality and privacy to mention some of these aspects. However, despite the evolution of this new model not as storage and data management features, doubts about its safety remain a concern.

Keywords—cloud, security, risk, confidentiality, privacy, cloud computing, security, vulnerability, standard, infrastructure, internet, paradigm, services, applications.

I. INTRODUCTION

In recent years, cloud computing has revolutionized the way the end user uses the Internet, but also service providers and online applications have benefited from the advantages of this technology. Moreover, regardless of the size of enterprises, the cloud computing offers generally and profitable applications and services easier to use, but it is essential to ensure that personal information and files are well protected. Currently the main challenge of cloud computing is that the user has no control over the infrastructure in which information is stored, however; there are numerous security problems for cloud computing as are many technologies involved such as: networks, databases, operating systems, virtualization, programming, among others; with own security problems solved [1].

A recent publication of the NIST (National Institute of Standards and Technologies) *"Guidelines on Security and Privacy on Public Cloud Computing"*, emphasizes the need to disseminate best practices on this model of service delivery, due to growing concerns about the security on these platforms [2]. In March 2010, the CSA published a report called *"Top Threats to Cloud Computing v1.0"*, in which he mentions the seven biggest threats facing infrastructure in the cloud, seeking advise companies and organizations to opt for these technologies. Likewise Gartner S.A. (he recognized research company and US consultancy in information technology with presence in 75 countries worldwide), made the report *"Assessing the Security Risks of Cloud Computing"* on the main risks to which companies and organizations with computer face on the cloud.

In this sense, the present research provides the result to perform a risk analysis of this infrastructure by using the Monte Carlo method, in order to represent different scenarios on the level of risk in adopting this technology.

II. CLOUD COMPUTING

There are several definitions for the term cloud computing; however according to the National Institute of Standards and Technology (NIST: National Institute of Standards and Technology), cloud computing is a model that conveniently allows on-demand access to ubiquitous networks to share a set of configurable computing resources (eg, networks, servers, storage, applications and services) that can be provided and release quickly with minimal management effort

or service provider interaction. This cloud model comprises five essential characteristics, three service models and four deployment models, as shown in Figure 1.

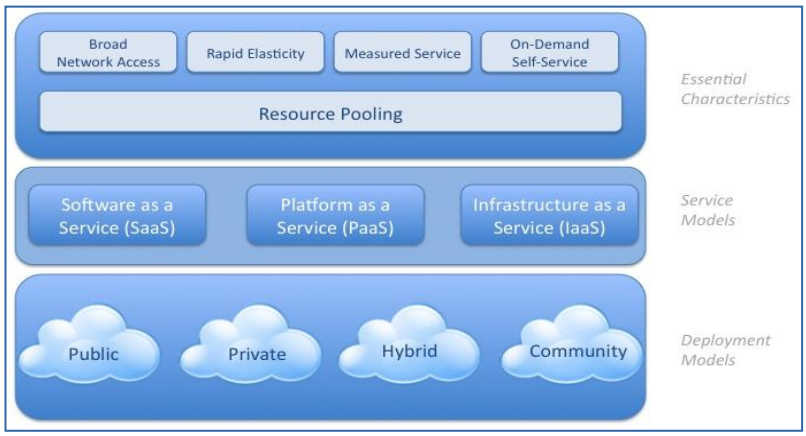

Figure 1. Model Cloud Computing, NIST.

Public clouds are fully hosted and managed by the provider, try to give consumers information elements uncomplicated case of software, application infrastructure, or physical infrastructure, the cloud provider takes on the responsibilities of installation, management, provisioning and maintenance. In addition to private clouds the user is responsible for setting up and maintaining the cloud. The difficulty and cost of establishing an internal cloud can sometimes prevent its realization. Also, a hybrid cloud is a combination of public and private clouds. Usually in these clouds management responsibilities are divided between the enterprise and public cloud provider.

When it comes to implementation, it is under the following schemes, taking into account the needs of the user. Software as a service, characterized by a complete application offered as a service, on demand, meaning a single instance of the software runs on the provider's infrastructure and serves multiple client organizations. Platform as a service, in this model of customer service is offered development platform and programming tools so you can develop your own applications and control application, but does not control the infrastructure. Infrastructure as a service, is a means of delivering basic storage and compute capabilities as standardized services on the network. Servers, storage systems, connections, routers, and other systems are concentrated (eg through virtualization technology) to handle specific types of workloads.

III. RISKS ANALYSIS WITH MONTE CARLO

Traditional systems are protected behind firewalls and a set of constraints, so that attackers must conduct a thorough intelligence work to access them; meanwhile the cloud services instead you are highly visible and are designed to be accessed from anywhere by anyone, a great white in question [10] .To perform a successful implementation of cloud computing, it is recommended to follow the following steps shown in Figure 2:

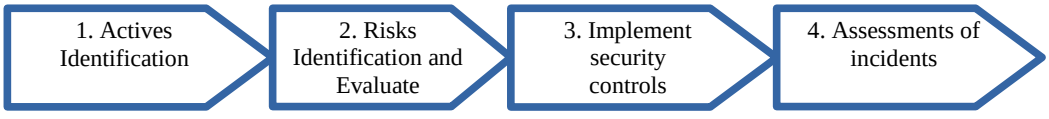

Figure 2. Steps for Risk Assessment

The process of identifying the goods takes into account both the consumer and the provider cloud need to identify the hardware and software assets. They should maintain and frequently update an inventory of assets that may change as a result of the restructuring of the company, more efficient

energy use and new legislation on export of data privacy across jurisdictions limits technologies. Depending on the needs of the consumer goods can be applications, operating systems, hardware, network infrastructure, among others.

To identify and assess the risks can be generalized to analyze how the main characteristics of information security (confidentiality, integrity and availability) [3] and those that complement (authentication, authorization and audibility) are affected. At this stage a performance organized by risk domains or layers of the model of cloud computing CSA was used. As it is shown in Figure3.

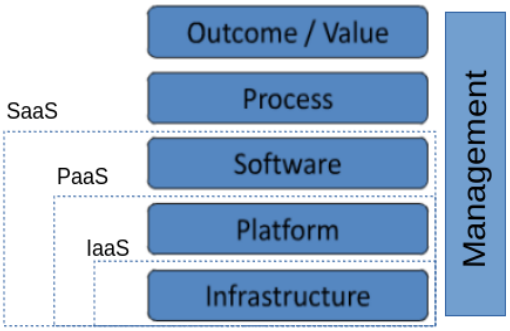

Figure 3. Cloud Computing Layers, CSA.

The next step in risk assessment is relatively simple in concept: applying security controls; however more difficult in real life to find out if the controls to mitigate risks are profitable, then the benefits outweigh the costs of implementing controls. In the application of controls it is important to maintain the relationship with the management system of information security and international standards on Cloud Computing, in that sense, and according to the CSA, a total of 95 controls were identified to take account, such as: whether the provider has the resources to continuity plans, use encrypted protocols, installing and configuring firewalls, review of policies and provider contracts, among others.

It assessments of incidents referred to the risk assessment should be conducted periodically since the risks may need to be reassessed more frequently if conditions such as the emergence of new technologies cloud service that can impact occurs software, hardware and network assets, emergence of new vulnerabilities and threats, new controls available that can effectively mitigate the risks., noticeable changes in legislation and compliance regulations in the various jurisdictions.

3.1. Monte Carlo Method

It is a quantitative method for the development of risk analysis. The method was named in reference to the Principality of Monaco, as "the capital of gambling". This method seeks to represent reality through a mathematical model of risk, so that randomly assigning values to the variables of the model way, different scenarios and results are obtained.

This method is based on making a sufficiently high number of iterations (value assignments randomly) so that the sample available results, is wide enough to be considered representative of reality. These iterations can be performed with the aid of a specific software for this method, for example: Risk, Crystal Ball, Full Monte, Gold Sim, Katmar and Risky Project. In this particular case we use the latter which is a risk management software. For the development of risk analysis based on measurement of the probability of occurrence, the steps are shown in Figure 4.

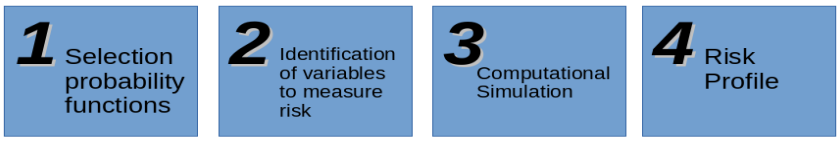

Figure 4. Steps to perform a risk analysis with Monte Carlo Method.

In the first step you need to identify the probability function that is associated with each of the affected variables for risk, that is, the function that explains and reflects the behavior of the risk variable; in this case a Gaussian distribution is used, which allows to consider all possible values regarding controls and risks involved.

During the identification stage of the variables, in this case our variables to consider are the total number of controls, total number of risks, net profit level of trust and value at risk (worst expected loss). In this case the last two are our output variables to study the implications in the project experienced variability in risk variables considered.

Once identified risk variables we want to know what is the behavior of those variables at the stage of the computer simulation, that is, what will be its range of variation for each of the scenarios.

We start by determining the probability that present each of the identified risks, determining the cumulative probabilities and ranges of these and a large number of random numbers we get values (which will represent the possible risks to be submitted) to be in a position calculate the mean, median and standard deviation. With the help of selected software (Risky Project) and the previously calculated data, the simulation begins, generating a million iterations in order to obtain a sample more representative of reality.

The results shows the risk model are possible to reach conclusions with the sample obtained from the different iterations made, which is representative of the fact same as shown in the graph of Figure 5.

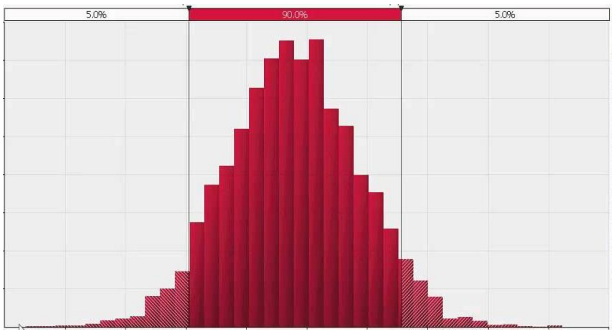

Figure 5. Graphic results of the simulation with Monte Carlo.

The graph is interpreted as follows: it is a technique to display all the results of the implementation of cloud computing considering the risks and probabilities of occurrence collected. The X axis is the whole range of values of the result and the Y axis is the cumulative probability of occurrence. It is much more risky implementation, the wider the range of possible outcomes, leading to a flatter curve. The more vertical is the representation, less uncertainty associated with it, so this representation allows us to identify who controls are required to cope with the risks that may arise, taking into account the features, layers, and type of cloud services deployed.

IV. FOOTNOTES

In terms of information security, economies of scale and flexibility offered by cloud computing can have a positive impact in the event that required less investment in security measures because the costs are distributed and may have negative impact because the massive concentration of resources and data become a more attractive target for attackers. In models of cloud computing, it is necessary to make an independent assessment of risks for each of the scenarios that can be implemented.

Moreover, since each consumer may require less or more controls depending on your needs, selecting our service provider in the cloud must be based on them, based on the direction you want for the company, the relationship cost-benefit, budget and rights and obligations under the contract, related to access, control and safety aspects of the information.

V. ACKNOWLEDMENTS

The Instituto Politecnico Nacional for give us the tools in the way of my professional training and all the teachers who were a guide during that time.

REFERENCES

[1] M. Ruiz. Seguridad de la computación en la nube. México, Distrito Federal:CINVESTAV IPN. 2013.
[2] A. Chacón, J. Hurtado. Definición de un modelo de seguridad de la información en nubes privadas y comunitarias. Santiago de Cali: Facultad de Ingeniería. 2012.
[3] H. Poveda. La nube de computación móvil: una solución a la demanda de procesamiento de señal en las comunicaciones móviles. Panamá, Panamá: Universidad Tecnológica de Panamá. 2014.
[4] B. Kezherashvili. Computación en la nube. Almeira: Universidad de Almeira. 2013.
[5] O. Ávila. Computación en la nube. México, Distrito Federal: UAM-I. 2011.
[6] J. Parada. Infraestructuras de seguridad en la nube. Madrid, España: Microsoft España. 2011.
[7] F. Pegrin. Cloud Computing: Privacy and Recommendations for the Use of Cloud Computing. Masachusets: 2011.
[8] K. Ryan, M. Kirchberg, L. Bu. From System-Centric Logging to Data-Centric Logging – Accountability, Trust and Security in Cloud Computing. Singapore:2011.
[9] K. Ryan, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg. A Framework for Accountability and Trust in Cloud Computing. Washington DC, USA:2011.
[10] K. Ryan, P. Jagadpramana, L. Bu. A File-centric Logger for Monitoring File Access and Transfers within Cloud Computing Environments. Washington DC, USA:2011.
[11] E. Bown. Final Version of NIST Cloud Computing Definition Published. Gaithersburg, USA:2011.
[12] J. Che, D. Yamin, T. Zhang, J. Fan. Study on the security models and strategies of cloud computing. Nanjing, China:2011.
[13] Y. Chen, V. Paxson, R. Katz. ¿What's new about cloud computing security?. California, USA:2010.
[14] J. Torres. Empresas en la nube: ventajas y retos del cloud computing. Barcelona, España:2011.
[15] A. Mento, A. Agarwal. Cloud Computing Service and Deployment Models: Layers and Management. Hershey, USA:2013.
[16] L. Martín, C. de la Torre. Valoración de Riesgos de un Proyecto utilizando el proceso Jerárquico de análisis. Universidad de Castilla,Toledo:2011.
[17] G. Dumrauf. Planificación y análisis del riesgo del proyecto. USEMA:2003.
[18] W. Jansen, T. Grance. Guidelines on Security and Privacy in Public Cloud Computing. Gaithersburg, USA:2011.
[19] M. López, D. Albanese, M. Analía. Gestión de riesgos para la adopción de la computación en la nube en entidades financieras de la República Argentina. Buenos Aires, Argentina:2013.

