Risk Assessment for Cloud Computing

Yogeshwaran Sivasubramanian
Department of Computer Science & Engineering
Amity University Dubai, UAE
syogeshwaran999@gmail.com

Syed Zubair Ahmed
Department of Computer Science & Engineering
Amity University Dubai, UAE

Ved Prakash Mishra
Department of Computer Science & Engineering
Amity University Dubai, UAE

***Abstract*—The broad implementation of cloud computing has brought a dramatic change to multiple industries, which derives from the development of the Internet-related technologies. Cloud service providers have untangled a lot of issues to maintain a robust quality of service. Despite the utilization of proficient techniques in resource management that has made optimal planning possible, as one resource is allocated to multiple users the risk of resources unavailability in cloud computing is still present. The level of risk is evaluated based on the probability of an incident occurring, which is mapped against the estimated negative impact. The probability of an incident occurring can be determined by the threat exploiting the vulnerability. All though a zero-risk scenario is impractical, effective risk assessment strategies equipped with efficient mitigation mechanisms can decrease the negative impact. As of now there are three types of cloud computing systems public, private and hybrid each with different levels of security. Most In this paper, we examine the various risk assessment models with regards to a Cloud Computing and touching upon Information Assets and Risk, Privacy and Confidentiality Concerns, Data Governance.**

***IndexTerms*—Cloud Computing,Risk Assessment,Risk Impact. Risk Management**

I. INTRODUCTION

Cloud computing provides the next era ofweb based, highly scalable distributed computing systems in which computational resources are offered ‘as a service'[1].Cloud computing has gained popularity due to its efficiency in delivering prominent results and reducing money on infrastructure and other expenses. Thus, most of the titans in the Technology field have invested into this technology. In the last quarter of 2016 cloud computing market was estimated at $148 billion. Such a huge market has fair share of security measures to keep all that content safe. The reputation of security concerns on the development and manipulation of information systems has never stopped growing. At present, Information Systems are utilized everywhere by individuals, organizations, governments and systems are target to information security attacks and it is very clear now that this would lead to a loss of a large amount of money, time and other resources.

The National Institute of Standards and Technology (NIST) defines risk management as “the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level” [3]. The NIST defines risk assessment as the process of identifying, estimating, and prioritizing information security risks which requires a careful analysis of threat and vulnerability information to determine the extent to which circumstances or events could adversely impact an organization and the likelihood that such circumstances or events will occur [3].

The probability security risk has a major impact on the consumers’ confidence to this software service. Quantitative security risk assessment models and other metrics can be used to reduce the odds of a risk occurrence and measure the security levels of their systems, products, processes, and readiness to address the security issues they are facing.

II. BRIEF VIEW ON CLOUD COMPUTING

Cloud computing has start to reshape the working IT environment in various industries but the general purpose remains the same. This purpose is well defined by theNational Institute of Standards and Technology(NIST) [4] as ‘‘a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services)that can be rapidly provisioned and released with minimal management effort or service provider interaction’’.

Cloud computing has been categorized in three major categories:

1. Cloud Infrastructure as a Service (IaaS)
2. Cloud Software as a Service (SaaS)
3. Cloud Platform as a Service (PaaS)

And four architecture modules have been established:

1. Private cloud
2. Community cloud
3. Public cloud
4. Hybrid cloud

III. RISK ASSESSMENT AND RISK MANAGEMENT

Risk assessment involves assessing the existing security and controls which includes the process of identifying the security risks to a system and determining their probability of occurrence, their impact, and the safeguards that would mitigate that impact. The main objective of risk assessment is to define appropriate controls for reducing or eliminating those risks [5].

As the occurrence of a risk not only affects the system but has an over impact on the business process as well depending upon the severity of the risk. In orderget a foreseen probability for the occurrence of a risk three methods can be taken into consideration:

- Qualitative Analysis Methods: Descriptive rankings are used to describe risk likelihood and impact.

IRJECE

- Semi-Quantitative Analysis Methods: Descriptive rankings are associated with numerical values.
- Qualitative Analysis Methods: Numeric values, for example, in the form of financial costs, are used to describe risk likelihood and impact

Risk management is the process of dealing with the business impact once a risk has occurred. The four primary responses are:

- Avoidance – Elimination of the cause of the risk.
- Mitigation – Reduction of the probability of occurrence or impact of that risk
- Transfer – Sharing of risk with partners eg: insurance.
- Acceptance – Formal acknowledgement of the presence of risk with a commitment to monitor it.

IV. RISK ASSESSMENT IN CLOUD COMPUTING

A general cloud computing infrastructure consists of a the cloud, the user, the devices the users uses to connect with the cloud and the identification method used to verify the device and the user. When we take only the cloud into consideration we see that there are primarily three places where risk can occur. One being compromised account, native malware on the application being used in the cloud or a data breach.

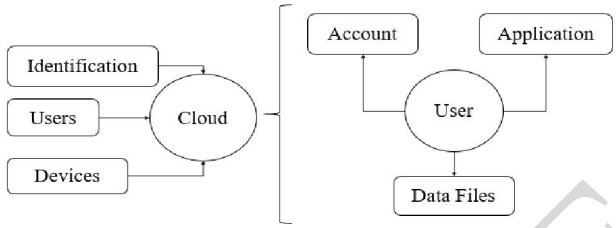


Fig 1. Basic Cloud Architecture

There a few risk assessment methods that available to us in the IT world, but as of now they have not been structured specifically for cloud computing environments. The risk assessment methods are as follows:

The Expression of Needs and Identification of Security Objectives (EBIOS)[7] is a methodology for evaluating and treating risks, which aims to determine the security actions to implement and also expressions safety.Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)[8] is a method of assessment of vulnerabilities and threats on the basis of the operating assets of the company. MEHARI [9] is a risk assessment method in the context of the security of information systems; this method is designed to meet the needs of each company.

These methods are applicable in a normal IT environment but there are more dynamics to a cloud computing environment which increases the complexity of risk assessment which these methodologies fail to cover effectively.

Simply taking into account either qualitative or quantitative analysis will not provide an accurate result. In the assessment of a complexinformation system, qualitative analysis and quantitative analysis should not be simply separated, on the contrary, the two methods should be integrated[6].

Quantitative risk and impact assessment framework based on NIST- FIPS-199 (QUIRC) focus on six key categories of security objectives (SO) (i.e. Confidentiality, integrity, availability, multi- party trust, mutual audit ability and usability)[10].The product of the probability of a threat occurring taken defined as quantitative risk i.e., an occurring threat event, and its potential impact or consequence. The threat event occurred would fall into one of the given SO category would be the average over the cumulative, weighted sum of n threats which map to that SO category[11]. This quantitative framework ranks the threat based on expert opinion about the likelihood and consequence of threats, as a scientific means to collect the information necessary for assessing security risks.

Blow table is a basic example how a risk could be measured in terms of impact, occurrence and disclosure. The tables contain fivecolumns (table 4). The first column contains the label of event or risk the next three columns contains the impact, occurrence and disclosure of the that risk. The product of these three categories is the Risk Priority Number (RPN) which is recorded in the fifth column.

Table I: To measure the impact of the risk

I-impact	Score
Barely Perceptible	1
Meaningless	2 – 3
Moderately Significant	4 – 6
Serious	7 – 8
Extremely Serious	9 – 10

Table II: To measure how often the rick can occur

O- Occurrence	Score
Unlikely	1
Very small	2 – 3
Small	4 – 6
Mild	7 – 8
High	9 – 10

Table III: To measure the risk disclosure

D – Disclosure	Score
High	1
Mild	2 – 3
Small	4 – 6
Very Small	7 – 8
Unlikely	9 – 10

RPN = I x O x D

RPN takes a value in the range 1 – 1000. The severity of risk determines the size ofRPN. The high value of the RPN has a great importance of risk.

Table IV: Example of quantitative risk assessment

Event/Risk	Impact(I)	Occurrence(O)	Disclosure(D)	RPN
Resource capacity	10	6	6	360
Unavailability of memory	9	3	8	216
Fluctuation in data transfer time	8	8	9	576

IRJECE

When taking the main aspects of cloud, data is the core asset that is getting stored in the cloud. In [11] they talk about effective data governance as a means to mitigate risk in cloud computing systems especially those issues related to data-ultimately offering many benefits to cloud consumers. They use the Otto Boris (2011) analytic theory for deducting and understanding the important processes necessary to construct an effective data governance design framework.

They have proposed a 5-step procedure for data governance as follows:
Step 1: Setup data governance structure
Step 2: Evaluate and assess existing data governance
Step 3: Setup data governance functions for cloud computing services
Step 4: Setup a negotiating contacts for cloud data governance
Step 5: Develop data governance level agreement

Though this is a much more targeted risk management method, it still requires further research and tailoring to catchup with the complexity of cloud systems. The problems that this methodology faces includes lack of funding for developing and deploying, technology, people and employee's skills and experience in this area of expertise[11].

The uncertainty aspects of cloud computing brings another challenge for risk assessment. The cloud being a dynamic system, it is hard to overlook the high level of complexity in providing solutions for problem. For example, programmers may not know in advance on what kind of resources are going to be available for their application in the cloud.Thus, programs should be developed for uniform and predictable virtual services, thus, simplifying their development [12]. Due to the process of virtualization in cloud it is impossible to know the exact information about system. Most of the time one resource is not dedicated to only one user, making it hard to predict the performance. If the job and processor characteristics and network's topology characteristics are known in detail (which is not the case in most cloud environments) then near optimal performance can be accomplished by scheduling the resource.

In [12] such uncertainties are grouped into parameter (parametric) and system uncertainties.Parameter uncertainties arise from the incomplete knowledge and variation of the parameters. System uncertainties arise from an incomplete understanding of the processes that control service provisioning [12].

The authors review various scheduling algorithms and methods for allocating resources and effectively handling unpredictable jobs that arise in the cloud system. The models attempt to provide the capability to dynamically allocate, manage resources in response to changing demand patterns in real-time, and dynamically adapt them to cope with different workloads and cloud properties to ensure quality of service[12].

V. CONCLUSION

Though cloud is a new technology there is an forever increasing need for it. Job scheduling and resource allocation in cloud environments are very dynamic in nature and difficult to predict. For that reason traditional IT risk assessment techniques prove to be ineffective in the cloud and the quality of service gets affected. Quantitative or qualitative assessment of risk in a cloud computing individually cannot provide accurate results but the integration of both would be much more effective. Few models proposed in the above discussed papers are theoretical and might be ineffective in a real-time environment. Though data governance can provide an overall view of the data being processed, it requires further research if the cloud is to hold big data. There is a need for a structured risk assessment method dedicated for cloud computing systems which can increases the trust between cloud users and cloud service providers.

REFERENCES

[1] Mohamed Al Morsy, John Grundy and IngoMüller An Analysis of the Cloud Computing Security Problem

[2] Peter Mell and Tim Grance The NIST Definition of Cloud ComputingVersion 15, 10-7-09 (https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf)

[3] Gary Stoneburner, Alice Goguen, and Alexis Feringa Risk Management Guide for Information Technology Systems NIST Special Publication 800-30 Recommendations of the National Institute of Standards and Technology

[4] Emam A.H.M. Additional Authentication and Authorization using Registered Email-ID for Cloud Computing. International Journal of Soft Computing and Engineering 2013; 3(2):110-113

[5] Survey: Risk Assessment for Cloud Computing by Drissi S. and Houmani H. and Medromi H.

[6] FENG Deng-guo, ZHANG Yang, ZHANG Yu-qing.Survey of information security risk assessment. Journal Of China Institute Of Communications,2004,7(25).10-18.

[7] EBIOS, Central Directorate for Information Systems Security, Version 2010 website. [Online]. Available: http://www.ssi.gouv.fr.

[8] Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), Carnegie Mellon - Software Engineering Institute, Juin 1999.

[9] Method Harmonized Risk Analysis (MEHARI) Principles and mechanisms CLUSIF, Issue 3, October 2004.

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

[11] Majid Al-Ruithe*, ElhadjBenkhelifa†, Khawar Hameed:

[12] A Conceptual Framework for Designing Data Governance for Cloud Computing The 13th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2016)

[13] Towards Understanding Uncertainty in Cloud Computing Resource Provisioning by TatjanaVasiljevaa, Sabina Shaikhulina, KarlisKreslins16th Conference on Reliability and Statistics in Transportation and Communication,RelStat'2016, 19-22 October, 2016.

IRJECE