European Journal of Computer Science and Information Technology
Vol.8, No.3, pp.1-8, June 2020
Published by ECRTD- UK
Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

RISK ASSESSMENT IN CLOUD COMPUTING

Varul Arora
Founder
TISEC
Belfast, Northern Ireland, UK
varul@tisec.io

ABSTRACT: *The primary purpose is to discuss the risk assessment in cloud computing and the issues which were tangled in multiple functional domains and to understand its current impact. This paper explores the following areas: cloud computing, characteristics of cloud computing, service models of cloud computing, risk assessment in cloud computing etc. There are many more areas, which can be explored in detail, where it can be used to generate better theoretical concepts and applications. This document will examine how the risk assessment methods of the cloud computing which are presently reoccurring over the Internet and discusses some of the issues with the Cloud Computing security features. This article presents some common elements for effective measures and outcomes***.**

KEYWORDS*:* cloud, cloud computing, risk assessment

INTRODUCTION

According to Microsoft.com "Cloud computing is the delivery of computing services – servers, storage, databases, networking, software, analytics and more – over the Internet ("the cloud"). Companies which can offer these types of the computing services are called cloud providers and typically charge for cloud computing services based on usage, similar to how we are billed for gas or electricity at home." [1]

Cloud services can be accessed through internet, which can lead to several attacks which may threaten the confidentiality, integrity and availability of data which is stored in the cloud. With the help of the intrusion detection system (IDS), detect and deter attacks can be monitored and the network traffic can be analyzed benefitting both the cloud provider and the security administrator. [2]

Environment and Fundamentals of Cloud Computing

A. Characteristics of Cloud:

The NIST (National Institute of Standards and Technology's) defines that the cloud computing should have the five characterisers which are essential, they are: -

- *Self Service on Demand:* - It provides the flexibility to customer to allocate the computing power without the help of the any human interaction.
- *Access of Large Network:* - It provides the availability of the cloud with the help of the client platform using the any type of network.

- *Pooling of Resources:* - Multi tenant model has been used by the cloud for serving its consumers. To maximize the number of customers, the resources have been pooled to increase the efficiency.
- *Measurement of service:* - With the help of the metering capability, cloud systems can monitor the usage and the type of the resources.
- *Instant Elasticity:* - The consumer has the capability for scaling rapidly outward and inward with proportionate to the demand. Also, the consumer has access of cloud services, any quantity at any time.

B. Service models:

According to the business of the consumer, the consumer has started its research and begin by determining the suitable service model for the selection of the cloud solution. The services proposed by cloud are as follows: -

- *SaaS (Software as a service):* - The users of this service can lease different set of applications running on the cloud by the provider. Example: - Amazon EC2, Windows Azure.
- *PaaS (Platform as a service):* - The users of this service can implement their applications on the cloud and run it according to their wish. Example: AWS Elastic Beanstalk, Windows Azure.
- *IaaS (Infrastructure as a service):* - The users of this service can lease a discrete infrastructure and run any kind of applications even the operating system as per their requirement. Example: - Digital Ocean, Linode,Rackspace.[7]

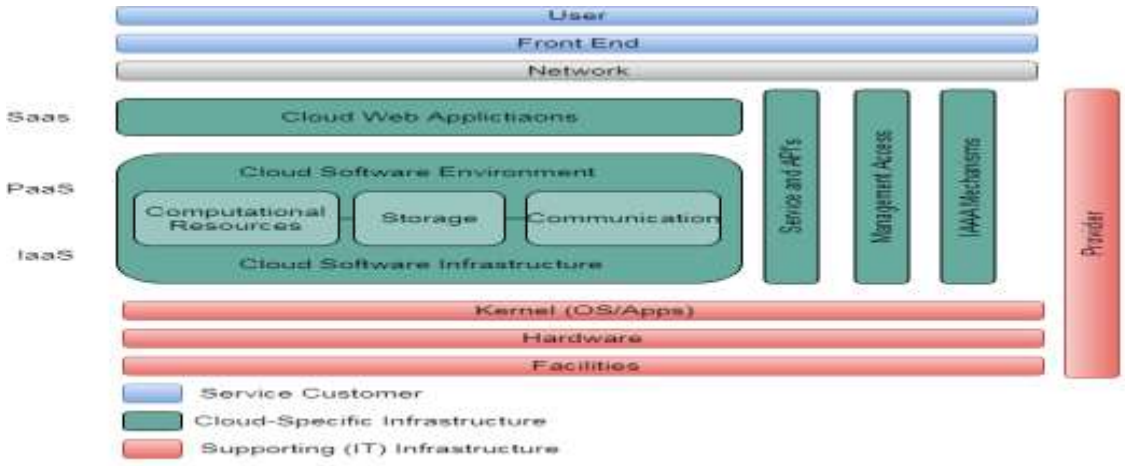

Figure 1 : The cloud reference architecture. We map cloud-specific vulnerabilities to components of this reference architecture, which gives us an overview of which vulnerabilities might be relevant for a given cloud service.

Deployment model:

After the service model, Deployment model succeeds. Deployment model is for the future consumer. The future consumer might think that how the consumer will get the benefit from the cloud and its services. Therefore, there are, 4 models for the deployment of the cloud: -

- *Private Cloud:* In private cloud, the system will be used by a single customer. The system can be maintained by the third party or by the client itself.
- *Public Cloud:* In public cloud, the cloud is deployed by a cloud provider for the client who wants the cloud services.
- *Hybrid Cloud:* The hybrid cloud is the composition of two or more deployment model.
- *Community Cloud:* In community cloud, the clients who share a common interest, will share the system. The infrastructure can be deployed in the client's location or it can be managed by the third party. [4]

Major Risk Issues in the Cloud Environment

Before moving forward in terms of determining the risks and g their reasons and factors, it is bifurcated in the three major terms that i.e. Threat, Vulnerability and Risk.

- *Threat*

A threat is an agent that causes harm to the target systems. Adware, Spyware, organised crime, malicious internal and Malware all are included in a threat. Viruses and worms are contained in a threat and can harm the system. The system tires to protect against the threats but the threats cannot be controlled.

- *Vulnerability*

Vulnerability is defined as a weakness/gap in a security program which can be exploited by an attacker to gain the unauthorized access of the system and cause damage. Vulnerabilities can be treated and detected. In a cloud environment, the vulnerabilities can occur in innumerable extent which may include network configurations, system platform, installed software and business operations.

- *Risk*

When the threat and the vulnerability overlap each other than the risk is formed. It means that the risk appears when the system has a vulnerability that an attack can be processed by a threat. [5]

Service Level Agreements

A SLA (Service Level Agreement) can be defined as a contract between its internal/external customers and the service provider that documents and defines the performance standards that the service provider is bind to satisfy. The SLAs as well as the security of the SLAs are a major emerging issue/hindrance in cloud computing. From SLA perspective, the studies, illuminated the question that how the cloud providers could address the security needs of the users in terms of integrity and confidentiality and also provided a detailed outline of the security controls. The cloud security service level agreement can be negotiated between the cloud provider and the users. As per the current scenario, the emergence of the cloud alliance to the worldwide market is an important part. Most of the researchers has induced the security service level agreements and allocated security metrics. Estimation and the calculation of the SLAs metrics are quite difficult. [8][9]

European Journal of Computer Science and Information Technology
Vol.8, No.3, pp.1-8, June 2020
Published by ECRTD- UK
Print ISSN: 2054-0957 (Print), Online ISSN: 2054-0965 (Online)

Risk Assessment of Security in Cloud

Risk Assessment Standards

There are several standards which are available for risk assessment. Some of them are *ISO/IEC 27002:2005, NIST risk management guide for information technology systems*, and" best practice" documents that are developed by security organizations, such as *CERT's OCTAVE method.* When we apply these standards to cloud, there are many unanswered questions such as How the security roles and responsibilities can be segregated, what are the activities needed to done by each role, What artefacts are generated by the roles in the cloud.

Motive and Limitation

The aim of the approach here being used is to provide a methodology of the security risk assessment that considers the probability of each and every threat which based on the real time data, also provides a feature of services conditional on the purpose of the user, and also providing multi-dimensional vulnerability measure in the perspective of the user. Visibility and controls can be obtained with the help of the transparent security, with respect to *security as a service.*

Assessing Model of Security Risk

When an asset, vulnerabilities and security threats intersect each other, then it is considered as a security risk. Risk of these kind cannot mitigate the user concerns of the security threats. Therefore, a new assessing security risk model is provided for user related threats *T* as follows: -

$$SR_T = \mathrm{N}_V \times [W]_S \times P_T \times [V]_T$$

To use the cloud service, NV the network vector is used. The probability of security threats is *PT*, and [*V*]*T* is defined as the vulnerability vector which is associated with security controls of cloud service providers. Here one more factor, [*W*] *S*, is added, which is priority of security controls in accordance with types of cloud service. In the table 1, the analysis of how the security threats and the corresponding security control is shown.

Table I. SECURITY TREATS AND CONTROLS

Security Controls		DL	ANU	ASH	API	MI
S	Data Isolation	•				
	Data Encryption	•				
	Data Location	•				
	Data Integrity	•				
	Data Back-up	•				
P	Application Isolation			•	•	
	Virtual Firewalls			•	•	
	Application Integrity			•	•	
N	Network Encryption			•	•	
	Traffic Isolation			•	•	
	Integrity Protection			•	•	
AC	Identity Management	•	•	•	•	•
	Access Management	•	•	•	•	•
	Key Management	•	•	•	•	•
AU	Logging	•	•	•	•	•
	Auditing	•	•	•	•	•
	Certification			•	•	
	Customer Privacy	•				

Define Security Threats and Corresponding Security Controls

Here the five threats have been considered form the top seven threats: Abuse and Nefarious Use of Cloud Computing (ANU, denoted to T1), Insecure Interface and APIs (API, denoted to T2), Malicious Insiders (MI, denoted to T3), Data Loss or Leakage (DL, denoted to T4), Account or Service Hijacking (ASH, denoted to T5). Therefore, an attempted has been done to match them to their corresponding security control which is an outlined framework for security mechanisms in service level agreements for the cloud services. The 5 threats have been categorised into Table 1 with their corresponding security controls: Secure Resource Pooling (Storage, Processing, and Networking), Access Control (AC), Audit, Verification, and Compliance (AU).

Security Threats Analysis

When the threat evaluation is considered, a multi-dimensional approach-based model is required. This means that not only the network environment and the technical factors should consider, but the service types should also be included.

Based on the network environment and technical factors in the cloud, the analysis of the security threats is done by, employing a 2 × 2 thinking matrix (Figure 2), which is used to facilitate better decisions and the thinking. The figure 1 is based upon two considerations with above mentioned five threats. The one is technical dependence, the other is uncertainty of threats.

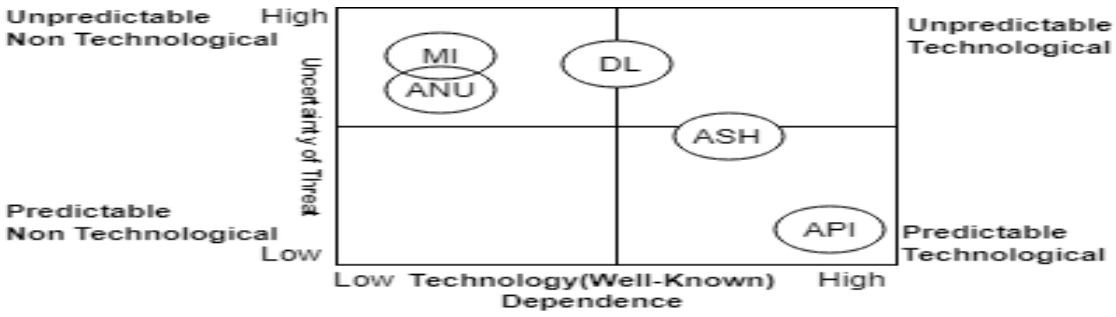

Figure 2: 2 x 2 Thinking Matrix of Threats

Since the AH, is the most predictable one and have the technical issue managed network such as internal network in cloud, in an untrusted network, it has high uncertainty of threats, for example public wireless network. This makes explicit statements about managing unpredictable aspects, for example, human resources, and natural disasters, untrusted network environments, etc. of security threats are the end of security controls.

Risk management in cloud computing

The first step in risk management is asset identification and establishing risk assessment. The potential risk identification could run after this assessment. A risk is the probability of cause of a problem when a threat triggered by vulnerabilities. The source of the problem is vulnerability and the problem itself is threats. Vulnerabilities are relevant to the security control and threats are related to the features of the asset. [10] ***A- Risk concepts:***

Any element that possess a value is defined as an *asset*. It includes tangible (software, hardware, personnel) and intangible assets (plans, organization, external factors, and technical factors). An *object* is called an asset in the risk process when there is an effect in the value of the object when the risk emerges. We can see the risk process in the figure 3.

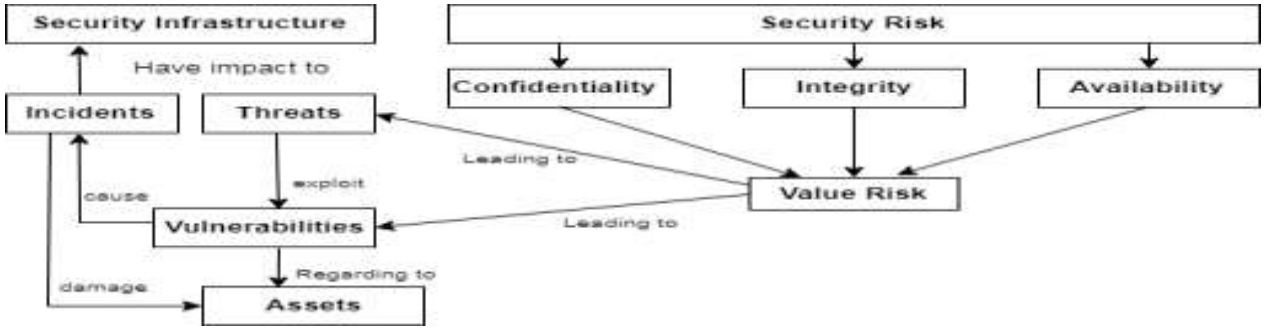

Figure 3 :- Risk Process

REVIEW OF RISK ESTIMATION METRICS

Simplest form:

Based on the 27005 standards, we can evaluate the risk by looking at the probability of successful attacks and the consequent severity of that attacks, should it occur. Risk (R) in the simplest form is the product between event probability P(E) and the possible damage, mostly described as an Impact (I).: ***R(E) = Pr(E) * I(E) (1)***

Where: R(E) = risk of an event, E = Event, P = Probability I = Impact.

Estimation of annualized loss expectancy ALE

We need to calculate it:

Asset Valuation (AV): Asset valuation is the process of distributing each and every information financial value.

Exposure Factor (EF): It is the value which is expressed within a range from 0 to 100 percent (%), that an asset's value will be destroyed by risk.

Single Loss Expectancy (SLE): It is the calculation of estimation of the monetary loss when a risk occurs.

The Single Loss Expectancy, Asset Value (AV), and exposure factor (EF) are related by the formula: *SLE = asset value (AV) x exposure factor (EF) (2)*

Next, we find *Annualized Rate of Occurrence (ARO):* Annualized Rate of Occurrence is the probability of risk that will arise in a specific year.

Annualized Loss Expectancy (ALE): It is the monetary loss expected annually for an asset due to a risk. It is determined by the two input values i.e.: the cost of the damage and the probability that the loss will occur. It's computed as follows: *ALE = SLE * ARO (3)*

Risk assessment by using Bayesian Learning Technique

which is explained as follows: -

According to *BSI PD-3002:2002* and Data-Centric

Quantitative Computer Security Risk Assessment research, the risk of an information system's asset could be determined by the following formula: ***Risk = Impact × Occurrence Rate × (Threat × Vulnerability).*** [6]

By using Bayesian Belief Network (BBN) we could determine the relationship between these factors and their probabilities to risk evaluation. According to the BBN diagram (which is shown in the figure 2 below):

P (Risk) = P (Impact) × P (Occurrence Rate) × P (Probability) (4)

P (R) = (P (Asset Value) × P (Classification)) × P (Occurrence Rate) × (P(Threat) × P(Vulnerability)) P (R) = (P (AC1) × P(AC2) × P(AC3) × P(AC4) × P(AC5) × P(C)) × P (ARO) × (P(T1) × P(T2) × P(T3) × P(T4) × P(V1) × P(V2) × P(V3) × P(V4))

AC1, AC2, AC3 are the factors which are related to asset value such as each asset could have one or more factors of the preceding. T1, T2, T3 are the common threats in the information system that could be categorized, according to BSI PD where as V1, V2, V3 are the vulnerabilities which are common from the similar guideline.[4]

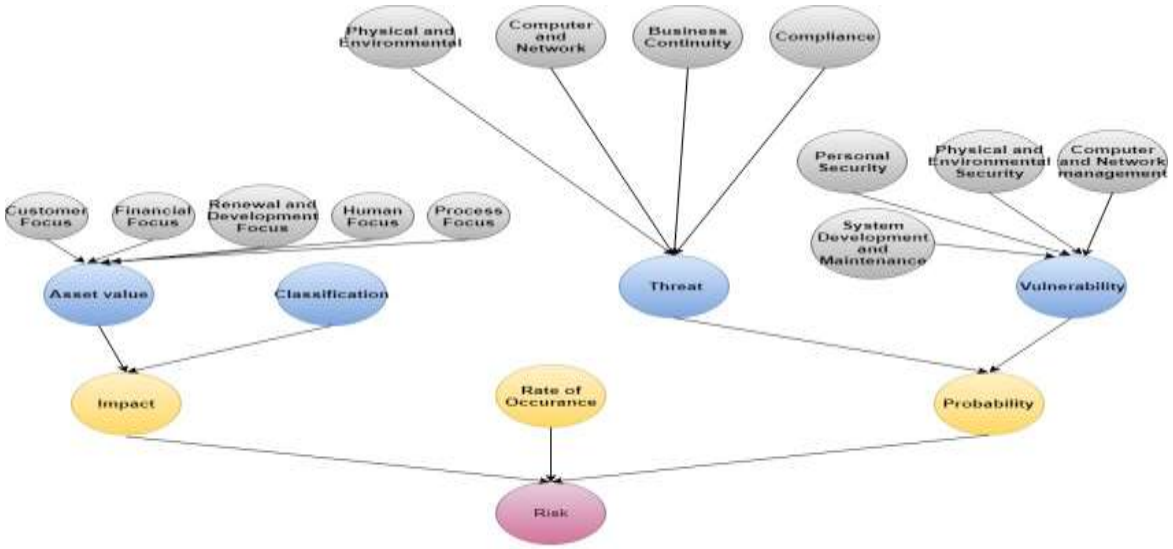

Figure 4 : Risk Assessment of Information Security Bayesian Belief Network

CONCLUSION

Cloud computing is a new emerging way in information and communication technologies. The use of traditional risk assessment models in cloud computing are inefficient due to its complexity and the use of distributed environment. This paper surveys and analyses several risks assessment methods in cloud computing from different perspectives. [3]. Further in this paper, we first discussed the main cloud computing characteristics and how these characteristics make difficult to apply these traditional security approaches.

Furthermore, this paper presents quantitative risk assessment of the cloud platform by defining relevant security metrics to support assessment process. Further we can see that, great attention has been given to the question that how security service level agreement could be assured and how the recommendation of the services could be given to users based on security service level agreements. Even though many researchers have suggested definitions and

evaluation models or processes for security service level agreements, quantitative security risk assessment for a user are rarely studied. A few approaches addressed quantitative model, not considering feature of security threats and services. Assessing security risk for security service level agreement might consider service types and usage environments, which influence to risk exposure in a user perspective. Cloud Computing is a suitable environment for all types of users especially for those who own a business environment. [8]

Lastly, in Cloud, every business owner/user of the services can choose the suitable model of Cloud to deploy his/her application in order to achieve the required degree of Quality of Service (for example:- service availability and integrity, cost saving, fast processing time etc.

REFERENCES

[1] What is cloud computing?,"https://azure.microsoft.com/en- gb/overview/what-is-cloud-computing/"
[2] Ben Charhi Youssef, Mannane Nada, Bendriss Elmehdi, Regragui Boubker "Intrusion detection in cloud computing based attacks patterns and risk assessment"
[3] Alireza Shameli-Sendi and Mohamed Cheriet, "Cloud Computing: A Risk Assessment Model" 2014 IEEE International Conference on Cloud Engineering.
[4] Amal Benfateh, F. Gharnati and T. Agouti, "ISA-based Model for Risk Assessment in Cloud Computing Environment."
[5] A. Chopra, P.W.C. Prasad, Abeer Alsadoon, S. H. Ali and A. Elchouemi, "Cloud Computing Potability with Risk Assessment."
[6] Noha E. El-Attar, Wael A. Awad and Fatma A. Omara, "Empirical Assessment for Security Risk and Availability in Public Cloud Frameworks."
[7] Mannane Nada, Bencharchi Yousef, Boulafdour Brahim, Regragui Bobker, "Survey: Risk assessment models for cloud computing: evaluation criteria."
[8] Karim Djemame,"A Risk Assessment Framework for Cloud Computing." IEEE Transactions on cloud computing, Vol.4, No. 3, July-September 2016
[9] Sang-Ho Na, "A methodology of Assessing Security Risk of Cloud Computing in User Perspective for Security-Service- Level Agreements."
[10] Mariam Kiran, Ming Jiang, Django J. Armstrong and Karim Djemame, "Towards a Service Lifecycle based Methodology for Risk Assessment in Cloud Computing." 2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing