2012

SLA-based risk analysis in cloud computing environments

Mohammed Almathami

SERVICE LEVEL AGREEMENT (SLA)-BASED RISK ANALYSIS IN CLOUD COMPUTING ENVIRONMENTS

By
Mohammed Almathami

Committee Members
Dr. Kaiqi Xiong (Chair)
Dr. Sumita Mishra
Dr. Yin Pan

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Computing Security and Information Assurance

Rochester Institute of Technology

Department of Computing Security
B. Thomas Golisano College of Computing and Information Sciences

Rochester, New York

November 2012

Rochester Institute of Technology

B. Thomas Golisano College Of Computing and Information Sciences

Master of Science in

Computing Security and Information Assurance

Thesis Approval Form

Student Name: Mohammed Almathami

Thesis Title: SLA-based Risk Analysis in Cloud Computing Environments

Thesis Committee

Name	Signature	Date

Dr. Kaiqi Xiong
Primary Advisor – R.I.T. Department of Computing Security

Dr. Yin Pan
Secondary Advisor – R.I.T. Department of Computing Security

Dr. Sumita Mishra
Secondary Advisor – R.I.T. Department of Computing Security

Thesis Release Permission Form

Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences

Title: SLA-based Risk Analysis in Cloud Computing Environments

I, Mohammed Almathami, hereby grant permission to the Wallace Memorial Library to reproduce this thesis in whole or part.

_____

Mohammed Almathami

_____

Date

Abstract

The cloud computing has been evolved in recent years which led many customers to utilize the cloud computing technologies. The research work in this area has spread due to many issues that have coincided with the vast growth of the cloud computing technologies. On the other hand, the cloud security concern has become one of the important issues that cloud computing introduces. One of the main components of cloud services is the service level agreement (SLA) that works as a contractual document between the cloud providers and their customers and states some metrics and parameters that must be enforced by the cloud providers or consumers. Despite various issues of the SLA in cloud computing, there is one issue that has not been discussed frequently in cloud computing security, which is the SLA in term of risk management. This research tends to perform SLA-based risk analysis in cloud computing environments. Moreover, it evaluates different SLA parameters such the risk factor, the response time factor, and the service cost factor. This paper also designates the importance of considering risk management as an SLA parameter in the negotiation stage between the provider and the consumer. However, it looks for the relation between those SLA metrics and risk factor associated with the cloud services.

Table of Contents

Dedication

I would like to dedicate this work to my beloved parents, Abdulaziz and Shahera Almathami. I would not reach this level of education without your caring support and influential help. For your sacrifices for me the whole time, I dedicate this work for you. I would like to dedicate this work to my brothers and sisters who keep encouraging me and always be happy about my achievements more than me. To my best friend Abraham, thank you for your influential help and your significant support.

Acknowledgement

I would like to give special thanks to my committee chair, Dr. Kaiqi Xiong, for his assistance and supervision through the thesis process. Thank you for your helpful suggestions and significant directions all the time. Also, I would like to thank my committee members Dr. Sumita Mishra and Dr. Yin Pan for your helpful suggestions and comments through the thesis process.

1. Introduction

Cloud computing has been one of the major emerging technologies in recent years. Cloud computing is based on delivering different services and resources through what is called the cloud or the Internet. These services differ from providing infrastructure resources to software services. Cloud computing depends on complex architectures that allow providers to deploy different models and deliver different services. One of the vast features that cause the spread of these technologies is the flexibility since these services and resources can be offered on-demand and the customer only pays according to usage. Also, they offer good scalable and elastic features to scale the existing resources to obtain extra resources and services on demand. Cloud computing consumers will not need to think about maintenance fees or software licenses since those operations will be taken care of by the cloud providers. Moreover, significant benefits of cloud computing such as cost effectiveness, portability, usability, and availability draw the attention of many consumers to use cloud services. Cloud computing services can be delivered in different models such as software-as-a-service (SaaS), which allows cloud customers to process and use licensed software on the cloud providers' resources only. For instance, the cloud consumers rent software such as human resources management system (HRMS) and run it in the cloud on the providers' resources. The cloud services can also be provided as platform-as-a-service (PaaS) which lets the consumers to rent only a platform that gives more control to the consumer to configure it as needed. The last model is infrastructure-as-a-service (IaaS), which provides the consumers with a complete infrastructure where they deploy different machines and storage resources. The cloud services can be deployed in different ways such as public cloud that allows all the consumers to share the same resources, private cloud that provides the consumers with detected resources, community cloud that allows two or more trusted consumers to share same resources, and hybrid clouds which allow consumer to combine the public and private clouds.

The features of cloud computing entice consumers to utilize the cloud services to improve the current computing services and save more money. On the other hand, the cloud security concern has

become one of the important issues that cloud computing introduces. Many IT leaders are afraid of moving to the cloud because of the security issues that arise from cloud computing technologies. One of the main components of using cloud services is the service level agreement (SLA) that works as a contractual document between the cloud providers and their customers. Cloud SLA states some metrics and parameters that must be enforced by the cloud providers or consumers. If any contractual party fails to meet any SLA requirements, that party commits a violation and is obligated to pay some penalties according to the SLA. Nonetheless, there are different areas in cloud computing that introduce new risks to both the cloud providers and customers. One of the issues that have not been discussed frequently in cloud computing security is the SLA in term of risk management. This research tends to perform SLA-based risk analysis in cloud computing environments. One of the strengths of this topic is that research evaluates different SLA parameters such the risk factor, the response time factor, and the service cost factor. The significance of the work conducted is to study the relationship between the risk management parameter and other SLA parameters such as response time and the cost. Also, since many SLAs lack security and risk management requirements, this research designates the importance of considering risk management as an SLA parameter in the negotiation stage between the provider and the consumer. The expectation consequences of this research are comparison results of the risk analysis against different SLA metrics such as stated response time and service cost. The research finds linkage between those metrics and risk factors associated with the cloud services. This topic is very interesting because it indicates some risk management issues with the current cloud SLAs. Furthermore, many IT leaders want to move to cloud but they face trust problem with the current ways of establishing cloud services' SLAs. Thus, this research gives those leaders some insights into the importance of risk management and how they should consider it while deciding the future cloud providers for them.

The remainder of this paper is constructed as follows. The next section provides background literature that relates to the research topic. Next, section 3 summarizes the research methodology used in this research. Section 4 then provides data collection and analysis for the SLA factors. Then, section 5

discusses the results of section 4 in depth. Some recommendations are provided in section 6 and the future work is provided in section 7. Then, the final part contains the conclusions of this research.

2. Literature Review

Several researches have been done in the area of SLA and risk management in cloud computing environments. Some of these researches tend to provide new SLA risk management models or frameworks to overcome security issues associated with the SLA in the cloud. This research focuses on an SLA-based risk analysis in cloud computing environments by examining three different SLA factors, which are the risk factor associated with the service, the service cost factor, and the response time factor. The related work in this area lacks research that concerns the SLA-based risk analysis and this may happen because the cloud computing security area has been one of the emerging research areas recently. The following parts discuss different research that has been done in the areas of SLA and risk management in the cloud computing environments.

In term of SLA-based work in cloud computing, Alhamad et al [1] proposed various models in this area such as an SLA-based trusted model for cloud computing. This model helps cloud consumers to evaluate the cloud resources and decides, which resources are more reliable to use. Moreover, Alhamad et al [2] also provided SLA framework for cloud computing. This framework provides good criteria that helps to build a good SLA in cloud computing and it discusses negotiation strategies between the cloud providers and other parties such as a cloud consumer, cloud broker, or SLA's monitoring agent. Hammadi and Hussain [3] proposed a monitoring framework for SLA. This framework helps third party providers to monitor SLA in real time to ensure that all parties meet SLA specifications of all time. This framework contains two modules: reputation assessment module and transactional risk assessment module and those two modules provide real-time QoS assessment to allow consumers to make a good decision by continue using the current service or moving to another service provider. Chi et al. [4] offered a data structure called "SLA-tree" to support SLA-based decisions in cloud environments. This structure contains two different data sets such as a waiting list of queries to be executed and the other set is an SLA for each

query, which points out different queries profits for modifying response times for each query. Jahyun Goo [5] proposed a framework for structuring SLA in IT outsourcing arrangements. This framework provides detailed descriptions of SLA measurement development and accurate statistical validations. This framework covers 11 SLA contractual factors and their relationships with three more sub-factors. This paper produced a benchmarking tool for SLA structuring efforts. Hedwig et al [6] proposed an SLA design for enterprise information systems. This design consists of different state-of-the-art concepts from system management and balances the risk with the process cost. This design helps IT leaders to understand the correlation between the process cost and the service quality. Bhoj et al [7] introduced architecture for SLA management in federated environments. This architecture uses SLAs to share selective information within different administrative boundaries. This helps federated clouds' consumers to share, measure, monitor, and ensuring the SLA specifications of the shared services. All those models and frameworks include and describe different SLA factors and metrics. The research chooses two of the most important factors: the response time and service cost. Those two factors have high impacts on making the decision about choosing the cloud service providers.

In term of risk management in the cloud computing environments, similarly, many papers proposed different frameworks in this area. Zhang et al [8] presented an information security risk management framework in cloud environments. This framework presents good insights in understanding the critical areas in cloud environments. It helps to identify threats and vulnerabilities and their impacts in the cloud environments. Furthermore, this framework discusses the possible actions needed to mitigate the risks. Yuqin and Helgesson [9] offered a modified risk management model by integrating the SLA to a pre-existing risk management model. This model clarifies the required responsibilities by various parties involved in the risk management process. Additionally, this paper presents a method to identify the relationship between risks and services and between services and actions. Morin et al [10] presented several issues and challenges of SLA and risk management in cloud computing. In this research, a risk management framework such as this framework [8] is used to identify and quantify risks in cloud computing environments.

In term of SLA-based risk assessment and analysis in cloud computing environments, the European Network and information Security Agency [11] presented a thorough report about risk assessment in cloud environments indicating that the SLAs force better risk management in cloud computing environments. Likewise, the Cloud Security Alliance (CSA) [12] indicates in its cloud security guide that cloud consumers should engage security departments in the establishment of the SLA so they can enforce some security requirements in the SLA. Research has been done in risk analysis in the area of cloud computing and SLA, in general. Yeo and Buyya [13] analyzed the resource management policing while accomplishing obligated objectives such as, meeting SLA, reliability and profit. This research uses two different methods for risk analysis: separate and integrated to identify the effectiveness of resource management policies in accomplishing the required objectives. Similarly, Waldman and Mello [14] discussed a framework for risk analysis of non-compliance with SLA requirements. This analytical framework discusses two different SLA issues: downtime and the number of failure occurrences. Moreover, Battré et al [15] presented a risk management process that can be used by grid providers to support SLA provisioning. The risk management process in this paper uses FERMA standard [16]. Also, risk analysis has been done to examine the relationship between the network availability and availability SLA specification [17] and this paper provides methods to control the risk and define availability SLA. Yang et al [18] presented a patch management framework based on SLA-driven patch applicability analysis, which allows automated analysis and risk assessment for business impact during the patch process. Patel et al [19] provided a mechanism to manage SLAs in cloud computing environments using Web Service Level Agreement (WSLA) framework to monitor and enforce the SLAs and they provided a real world scenario to evaluate their proposal. Moreover, Hovestadt et al [20] offered a workflow for selecting the best cloud resources according to the assessed risks and they provided some measurements to calculate different factors to support this workflow. Previous research did not relate or analyze information security risk against SLA metrics and specifications as this research intends to do. In term of the different techniques that have been used in the previous research, several researches in the area of SLA risk management in cloud computing are just providing general frameworks and models to

implement the risk management process. Furthermore, most of the risk analysis researches did not implement the research scenarios and they did not even simulate them such as Hovestadt et al [20], which presented risk analysis based on assumptions. Also, Yeo and Buyya [13] focus on the grid environments and they have simulated their environment using GridSim [21] and for cloud environments, it would be better to use CloudSim [22] to simulate cloud environments. Nonetheless, this research cannot use CloudSim to simulate the test environment due to some limitations in this toolkit regarding response time calculations and risk estimations. Correspondingly, Waldman and Mello [14] used the state of art model and assumptions to evaluate the risk of non-compliance with SLA requirements. However, this research does not match or relate the risk factor with other SLA factor such as the cost or response time. Yeo and Buyya [13] claim that the work was able to determine the performance difference in resource management policies against a single SLA object or combination of the objects. Moreover, this paper presents decent workflow to select resource according to assessed risks and it provided good methods to do the measurements and this could be used to calculate the risks and decide the best cloud resource. Waldman and Mello [14] state that risk of lack of availability is an essential parameter for the elaboration of SLAs.

In brief, most of those researches discuss the subject of SLA and risk management in general. For example, some papers perform risk analysis for SLA as a general concept such as [20] but in grid communication not cloud computing. Also, some papers discuss different SLA factor such as availability in this paper [17]. Thus, to the best of our knowledge, there is no research has been published that performs SLA-based risk analysis for the three SLA factors in cloud computing environments, which states the significance of this work. Also, this research is considered a significant work because it implements and analyzes SLA-based factors in a real test environment. Since this environment provides us with real-time measurements, the research provides factual outcomes. Moreover, this research studies the relationship between the SLA parameters: response time, cost and the risk factors. This research also declares the importance of including risk factor as an additional SLA parameter in the negotiations between the cloud providers and other parties

3. Methodology

This research studies three different factors: service response time factor, service cost factor, and risk factor. To acquire the calculation of the three factors, a performance study is done to evaluate the response time of different cloud resources. Then, the response time's result is compared to other results received from evaluating the service cost and associated risk with each cloud resource. Then, the risk analysis results help us to produce different charts that depict the relation and correlation between the three factors.

Before explaining how to calculate each factor, the research scenarios that are implemented to achieve the research objectives are stated first. In this scenario, an external private cloud environment is implemented in Amazon AWS. The cloud environment contains different virtual machines that build a complete and isolated private cloud in Amazon Virtual Private Cloud (VPC) and the environment topology is depicted the cloud setup later in this section. The scenario starts with one virtual machine (VM) in this cloud. Next, different tests are performed to gather the results of the average response time, service cost, and the associated risk. Then, the VMs are increased by one and same calculations are performed against all existing cloud resources. The scenario has up to 10 VMs in total.

Figure 1 clearly depicts the network design and configuration of the experiment. To establish the cloud environment, the virtual private cloud is created using Amazon VPC in the US West (Oregon) availability zone [23]. This zone has all the VMs that the tests are run against. First, the first VM is created and the calculation is done for all factors against one VM. Then, one VM is added and the calculation is performed for each VM. In addition to test server runs from RIT, another VM is acquired in another Amazon availability zone (EU Ireland) for testing purposes.

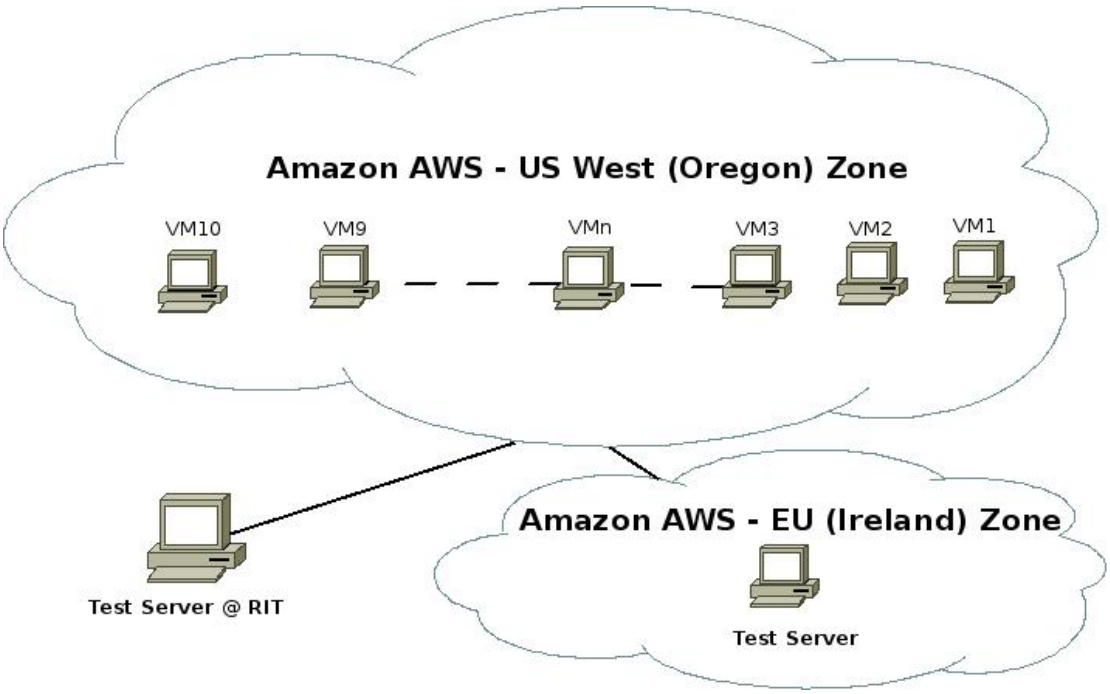

Figure 1: Virtual private cloud topology

In the following sections, the three SLA factors are listed and how those factors are calculated:

Response Time:

The response time is the time period between initiating request and receiving the response. The response time testing in cloud environment helps to provide better cloud resources provision process where customers make sure that they receive decent services as declared in the service level agreement (SLA). This test also assists to examine the availability of the cloud resources since cloud services should be available 24/7 when needed. In this case, this helps to find the relationship between the response time factor and risk factor in cloud environments. In cloud environments, when more cloud resources and Amazon instances are being added, do the added resources or Amazon instances affect the risk factor? This task aims to find clear answers using various test cases to verify whether the risk factor is essential or not. Since the environment is built in Virtual Private Cloud (VPC) in Amazon AWS in the US West Oregon availability zone, different tests are performed within the VPC and outside the cloud. Those tests use Perl client-server codes where the code is placed on each VM to listen on a specific port. On the other

hand, the testing server initiates multiple TCP packets and sends them recursively to each VM. Then, the code calculates the round trip time between the testing server and each VM. While adding more VMs, the server keeps sending the packets to the new VM and calculates the average response time the VMs. For each VM, the test server sends 100 packets and finds the average of the response time that it receives from each VM. In this part, the response time is evaluated from three different physical locations: same subnet, another Amazon availability zone, and from RIT campus.

On the other hand, end-to-end delay response time test is performed between all VMs. In this case, this study assumes that a customer initiates a service request and that request passes all the cloud resources. The response time needed to pass all the VMs is calculated. The first case is to assume that the last cloud recourse executes the request while the second case requires the last cloud recourse to respond to the customer with some feedback.

Service Cost:

In this metric, this research examines how the cost factor can be exaggerated in cloud environments while utilizing more cloud resources. One of the main benefits of cloud environments is to use less physical resources and utilize more virtual resources. In general, the cloud environments reduce the IT expenses due to cutting the cost of physical resources, manpower, maintenance and operations.

Risk Factor:

In this part, the research uses the information security risk management framework [8] to calculate different risks associated with each VM. This framework helps us to do risk assessment for this study scenario by following some standards. This part aims to identify the level of risks associated with each VM in cloud environment. After the risk analysis results are acquired, the charts are created to illustrate the risk behavior in this study scenario. More detailed steps of the risk assessment and all formulas are provided in section 4.3.

4. Data collection and analysis

4.1. Response time factor analysis

Amazon does not clearly state its average response time for Amazon EC2 instances to respond to a network request. It only claims that any instances opened through console will respond in a high manner [24]. To acquire the response time for each VM, this research performs three different test cases as the following:

4.1.1. Response time test within the same VPC subnet

In this case, this study runs a response time test within the same subnet of the cloud infrastructure. It launches a VM for testing in the same Amazon availability zone (US West Oregon). Then, the test server performs a response time test and sends the TCP testing packets. In average, the test server has sent about 100 packets per VM. Table 1 illustrates the average response time results while increasing the VMs one after another:

VM#	IP	Average Response time (Millisecond second)
1	10.10.10.50	0.446832
2	10.10.10.51	0.363171
3	10.10.10.52	0.282536
4	10.10.10.53	0.438948
5	10.10.10.54	0.429387
6	10.10.10.55	0.425957
7	10.10.10.56	0.371176
8	10.10.10.57	0.407007
9	10.10.10.58	0.429922
10	10.10.10.59	0.440493

Table 1: Average response time within the subnet

Figure 2 shows the fluctuation of the response time factor. First, it has a minor drop at the beginning of the test. Then, the response time goes up until it remains steady for a while. Then, the response time of a VM within the subnet becomes constant, yet there is no clear reason for the first drop except the network connection delay.

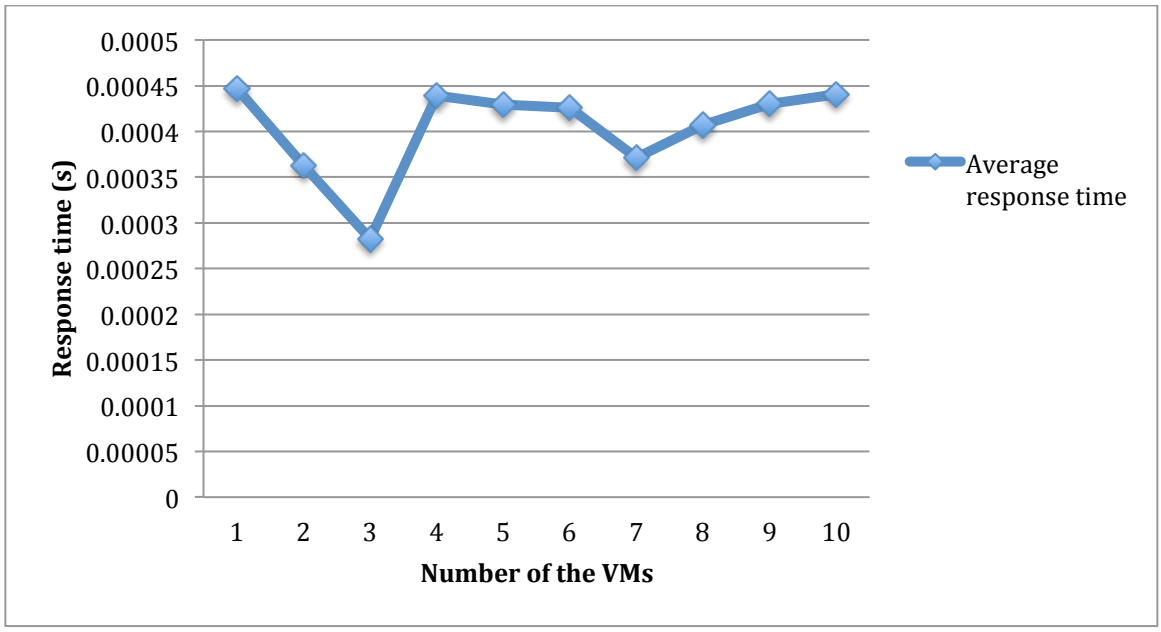

Figure 2: Average response time within the subnet

4.1.2. Response time test from different Amazon availability zone

In this test, the test server performs a test within the Amazon datacenters. Another VM is set up in a different availability zone, which is the Amazon Europe datacenter in Ireland. This test helps to find the response time between two availability zones at Amazon AWS: the US West Oregon and EU Ireland. Like the previous test, the test server sends multiple TCP packets and finds the average response time of each VM. To access the VMs, a public IP is associated to each VM so it can be publicly accessed. Due to the limitation of the VPC services at Amazon AWS, Amazon limits the cloud to use only five public IPs in each availability zone. Accordingly, the five IPs are kept switching between the 10 VMs. Table 2 illustrates the test results while increasing the VMs one after another:

VM#	IP	Average Response time (second)
1	50.112.141.143	0.171669144
2	50.112.133.99	0.172128291
3	50.112.141.143	0.169796751
4	50.112.141.159	0.168599153
5	50.112.141.158	0.168717644
6	50.112.141.105	0.169784105
7	50.112.133.99	0.172184668
8	50.112.141.143	0.170136806
9	50.112.141.158	0.169683541
10	50.112.141.159	0.169808068

Table 2: Average response time from other Amazon availability zone

Figure 3 depicts the response time factor behavior when this study tests the private cloud from another available zone at Amazon. It is clear from the chart that the response time factor has a dramatic decrease at the beginning. Later, the response time has fluctuated for the remaining part of the test and fluctuation is around average response time of 0.17 second. The possible reason for this behavior can be explained as the connection spends more time to be constructed between two availability zones.

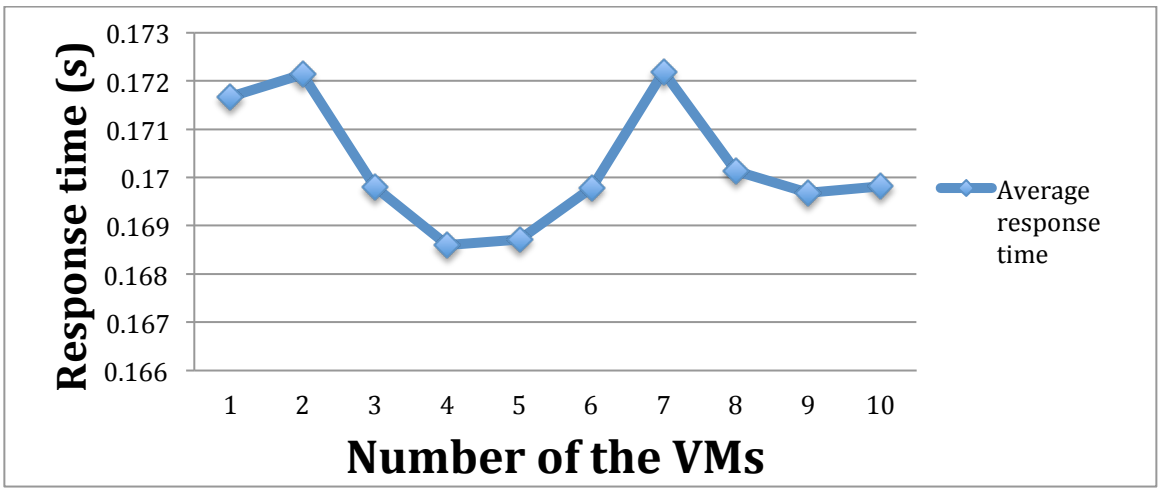

Figure 3: Average response time from other Amazon availability zone

4.1.3. Response time test from RIT network

In this test case, the test server performs a test from RIT network in Rochester, New York. This test helps to examine the response time between the customer network and the cloud resources over the Internet. It shows how the connection performance is an important factor when a customer may decide to move to cloud environments. Similar to the previous case, there are only five public IPs that can be associated with the VMs. Thus, the five IPs are exchanged between the VMs to perform the test. Table 3 illustrates the test results while increasing the VMs one after another:

VM#	IP	Average Response time (second)
1	50.112.141.143	0.09251992799
2	50.112.141.105	0.09008345127
3	50.112.133.99	0.08998443381
4	50.112.141.159	0.09228640373
5	50.112.141.158	0.09050016762
6	50.112.141.105	0.08957309722
7	50.112.133.99	0.08996924911
8	50.112.141.143	0.09210723337

9	50.112.141.158	0.09455870107
10	50.112.141.159	0.09595080172

Table 3: Average response time from RIT

To illustrate the response time behavior while connected from RIT, Figure 4 indicates a fluctuation in response time between 0.089 to 0.092 second. Then, the response time went up significantly while adding more VMs. This behavior demonstrated that adding more VMs could affect the response time factor based on the physical location of the new VMs.

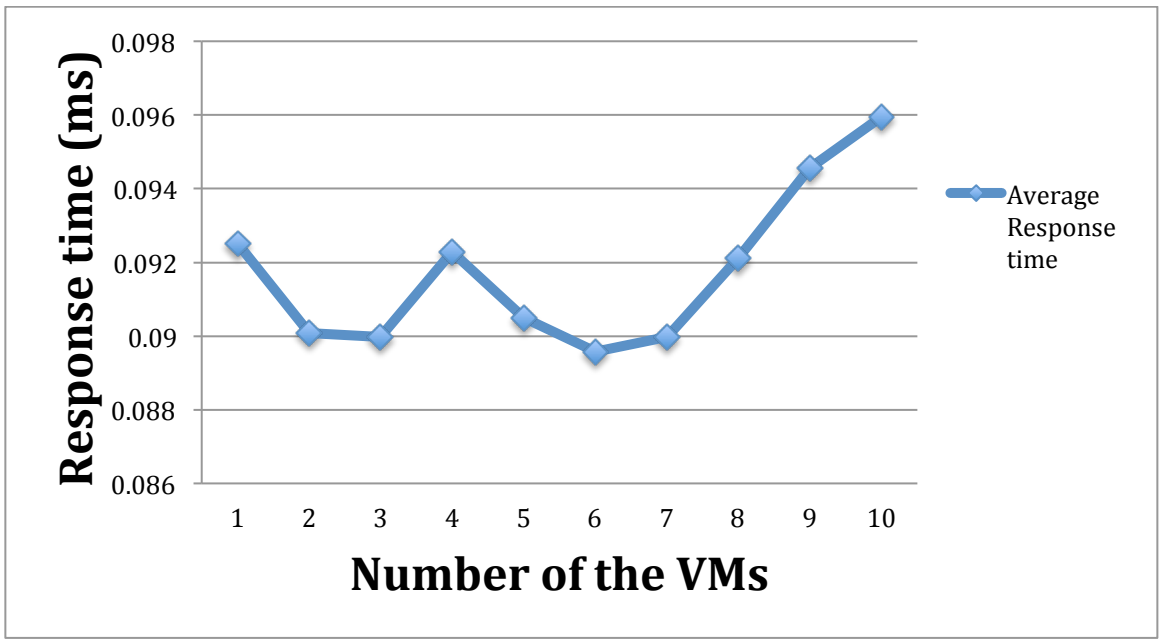

Figure 4: Average response time from RIT

To compare between the test cases, Figure 5 shows the enormous difference between the subnet case and other cases. Connecting within the subnet cannot compare to the connection outside the private network. Thus, interactions between the cloud resources at the same subnet are considered very fast and provide better cloud resources availability. On the other hand, the response time for the Amazon availability zone and RIT test cases are slightly close and have the same fluctuation around 0.17 seconds for the Amazon and 0.91 seconds for the RIT case. Moreover, the comparison illustrates that the connection from a regular US network, such as RIT, is faster than the connection from Amazon datacenter overseas (Ireland) to the VMs in US. Even though Amazon provides high-speed connection

between all its datacenters, the physical location of the datacenters play an important role since the other datacenters help in term of data recovery, business continuity, and backup process. Beside the response time factor effect, using multiple datacenters help to reduce the risk of data loss and cloud resources availability. Figure 5 depicts the average response times of each case are almost constant with minor fluctuations at some points. Thus, this chart declares that placing the VMs at the same physical machine and same availability zone would provide a constant response time for each VM.

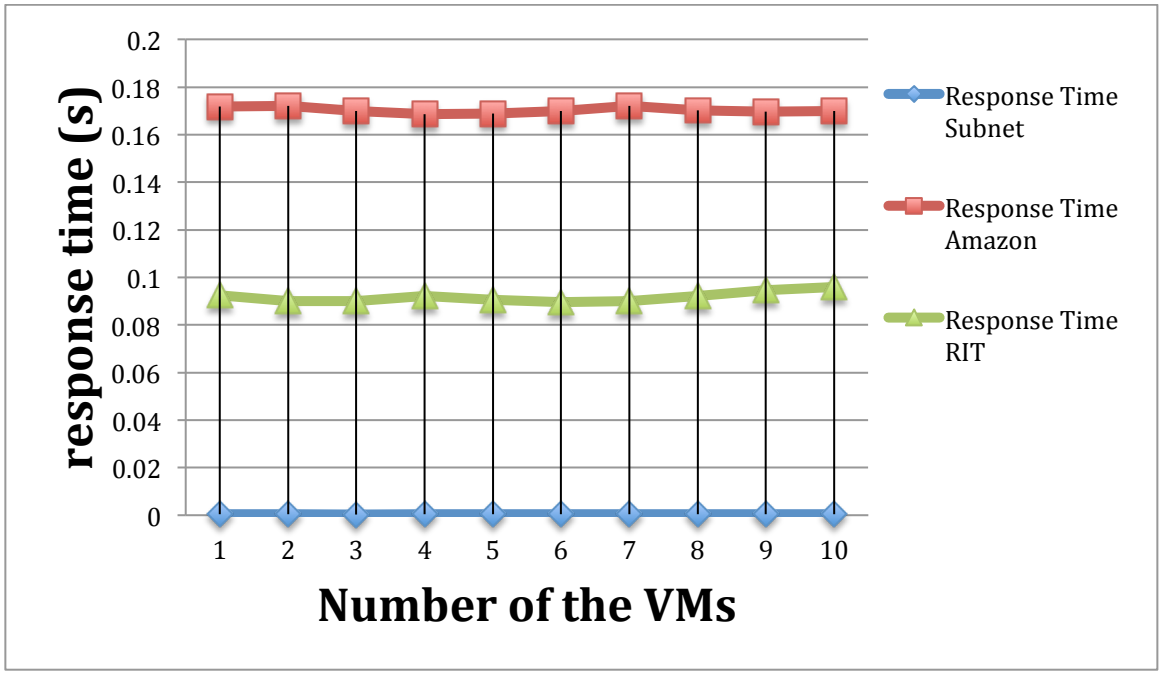

Figure 5: Comparison between the test cases

4.1.4. End-to-end response time delay between the VMs:

In this test case, this study assumes that a customer issues a service request that goes through each VM consecutively. The customer requests a service as illustrated in Figure 6, then, the request goes to VM #1. Next, the request is sent to VM #2 by VM#1 and so on until the request reaches the VM #10. After the last VM executes the request, VM #10 either responds to the customer or exits the process.

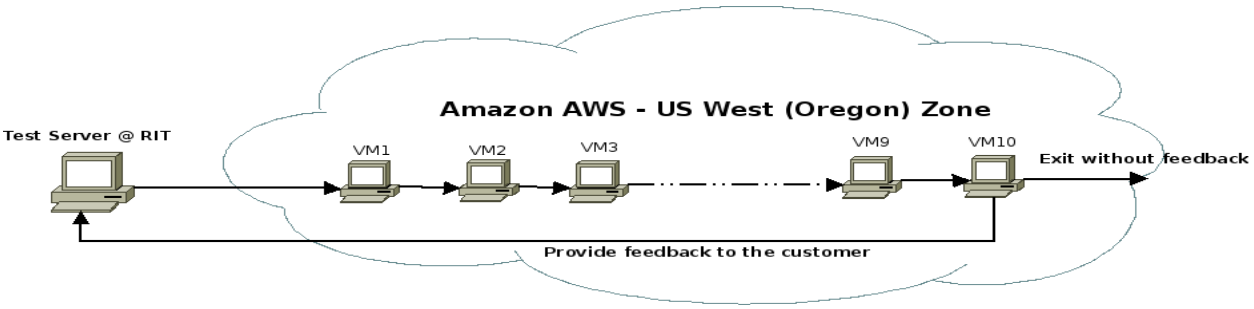

Figure 6: End-to-end response time delay for a service request

In this part, this study aims to calculate the response time that a request takes from the customer network until it executes by the last cloud node i.e. VM #10 in this case. In this calculation, the study assumes that the request has different process time at each VM. Thus, the response time between the cloud nodes in this scenario is only calculated.

VM#	Request Source	Request Destination	Average Response Time (second)	$\sum_1^i$ Average response time of a request
1	RIT (129.21.145.248)	VM1 (50.112.153.2)	0.07328167828	0.07328167828
2	VM1 (10.10.10.50)	VM2 (10.10.10.51)	0.00041709524	0.07369877352
3	VM2 (10.10.10.51)	VM3 (10.10.10.52)	0.00037762613	0.07407639965
4	VM3 (10.10.10.52)	VM4 (10.10.10.53)	0.00044880732	0.07452520697
5	VM4 (10.10.10.53)	VM5 (10.10.10.54)	0.00037919998	0.07490440695
6	VM5 (10.10.10.54)	VM6 (10.10.10.55)	0.00049640915	0.0754008161
7	VM6 (10.10.10.55)	VM7 (10.10.10.56)	0.0003716199	0.075772436
8	VM7 (10.10.10.56)	VM8 (10.10.10.57)	0.00035345077	0.07612588677
9	VM8 (10.10.10.57)	VM9 (10.10.10.58)	0.00037232553	0.0764982123
10	VM8 (10.10.10.58)	VM10 (10.10.10.59)	0.00036345005	0.07686166235
RIT	VM10 (10.10.10.59)	RIT (129.21.145.248)	0.07356992959	0.15043159194
Average response time of a request				0.15043159194

Table 4: End-To-End response time delay between the VMs

To analyze the data in Table 4, the research assumes two different cases: the first case is to consider the request needs to be sent by the customer to the cloud resources. The request passes each VM until the VM # 10. Then, the VM #10 does not need to take any action and the research assumes the request has been fulfilled. Figure 7 shows that response time of a request that finally fulfilled by VM #10. The change in the response time is steady increasing while adding more VMs.

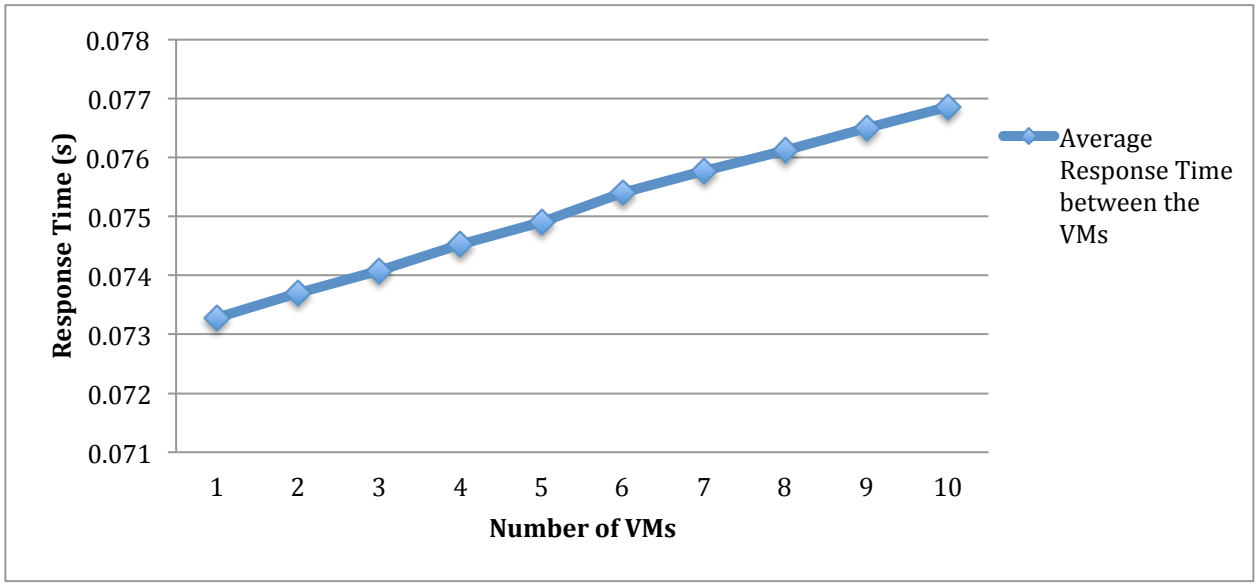

Figure 7: Average response time delay between the VMs

The second case is to assume that the last VM #10 responds to the customer. In this case, this study calculates the response time between the last VM and the customer network. Figure 8 clearly illustrates the important effect in response time when the last VM responds to the customer request. A sharp increase the response time after VM #10 indicates the enormous impact in the performance if the service provider decides to respond to the customers. Thus, processing the request inside the cloud would need minimal time besides adding final response time to the customer. Moreover, this behavior states the importance of considering the response time between the external network and cloud network; this includes the responses to the customers who are located in an external network.

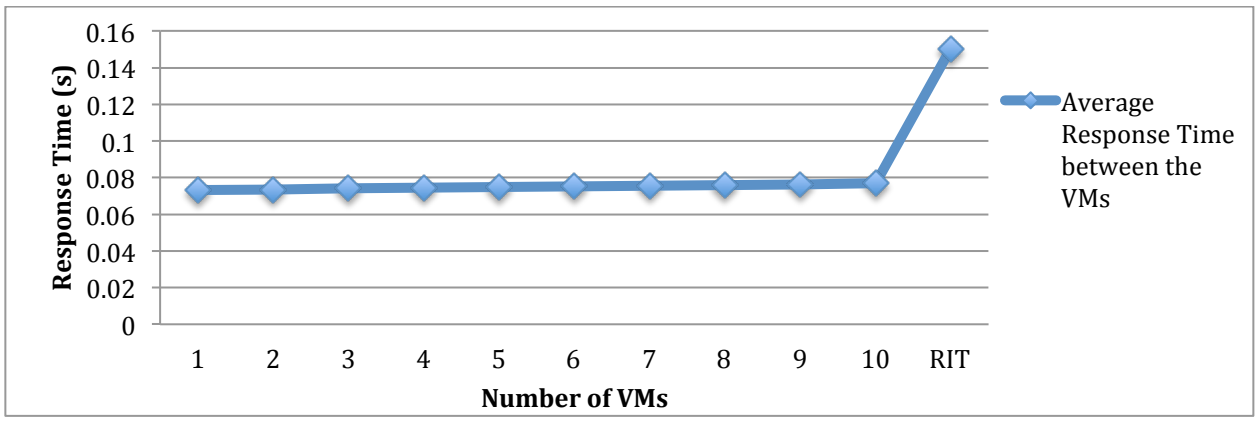

Figure 8: Average response time delay between the VMs including RIT

4.2. Cost factor analysis

All the cloud resources costs in this analysis are acquired from the Amazon AWS pricing policy [25]. There is no minimum fee required and the price depends only on the hourly usage. All the used Amazon instances are on-demand instances, hence; the test is charged for the usage time only. Additionally, all prices are based on the availability zone, which is the US West Oregon and all the VMs are Small type. The following table shows how the cost factor keeps increasing while adding the VMs successively:

VM#	OS	Price per Hour	Subtotal price per Hour
1	Linux	$0.080	$0.080
2	Linux	$0.080	$0.160
3	Linux	$0.080	$0.240
4	Win	$0.115	$0.355
5	Linux	$0.080	$0.435
6	Win	$0.115	$0.550
7	Linux	$0.080	$0.630
8	Win	$0.115	$0.745
9	Win	$0.115	$0.860

10	Win	$0.115	$0.975

Table 5: Cost factor behavior

Figure 9 depicts the cost factor behavior. The cost factor rises gradually when while adding more cloud resources. Nonetheless, the chart indicates how cloud environment can be incredibly cost effective. For instance, the test cases contain 10 servers that run for an hour and the total cost for all test cases is almost one dollar.

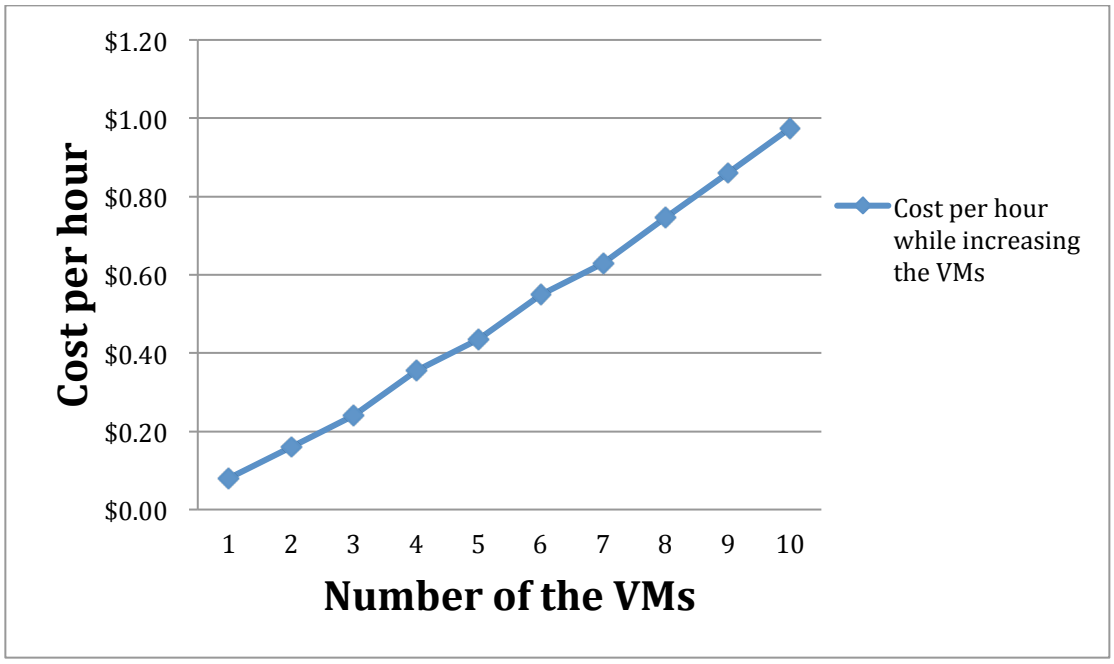

Figure 9: Cost factor behavior

4.3. Risk factor analysis

After finishing the response time and cost analysis in previous part, here is the risk factor analysis of the scenario. First of all, National Institute of Standards and Technology (NIST) defines the IT risk as "the net mission impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) particular information system vulnerability and (2) the resulting impact if this should occur" [26]. This task is proposed in a standard quality cycle based on ISO/IEC 27001 standards [27]. This cycle includes four main steps: Plan, Do, Check, and then Act. Next part is the risk analysis for this study scenario using the previous cycle:

4.3.1. Information Security Risk Management Program (PLAN)

4.3.1.1. Select the critical areas

In this part, this research uses list provided by the CSA on the critical areas of focus in cloud computing environments [12]. The main critical areas in this study scenario would be:

- **Governance and Enterprise Risk Management:**

This domain is considered one of the most discussed area in cloud computing. Since the cloud computing tends to restore more administrative roles and permissions from the cloud customer, the cloud providers have the responsibility to govern the cloud services and provide reliable and trustworthy services to build the trust relationship between the cloud providers and their customers. Also, the cloud providers are accountable to measure various risks introduced by cloud computing and how customer can transfer this task to the cloud provider. For this study scenario, this area is very important since this study tends to set up the private cloud in external and shared infrastructure i.e. Amazon cloud services. This research examines how Amazon govern the cloud and perform risk management tasks and it gathers this information from Amazon documents such as Amazon Web Services Risk and compliance document [28].

- **Information Management and Data Security:**

This area is also an important factor, since this study is using shared resources from a public cloud provider such as Amazon. This research aims to ensure that a managing data process is being built in the shared infrastructure to protect the data while using the cloud. Even if this study scenario is designed as a private cloud, there is no physical control over the data since all the data is transferred to Amazon datacenters. This research also aims to ensure that Amazon has designed good security controls to manage the data. This process identifies who is accountable of the confidentiality, integrity, and availability of the data and the VMs. This study measures the risks introduced to the study scenario by including this area.

- **Encryption and Key Management:**

Since the private cloud is placed in Amazon, a remote access is required to access the VMs and perform regular tasks. In the risk analysis, the research measures the risks associated with this factor. It examines how the connection to the VM is well protected from any adversary. This is based on the current encryption and key management controls provided by Amazon.

- **Virtualization**:

Virtualization is considered one of the most risks associated with cloud computing. Since the first time the cloud has been introduced, the virtualization remains the first security issue that introduces various risks to cloud provider and customers. There are different factors that virtualization uses to provide cloud services such as multi-tenancy, VM isolation and hypervisor vulnerabilities [12]. Also, this study aims to examine how the virtualization risk concerns may affect the VMs in a shared environment.

4.3.1.2. Strategy and planning

The ultimate goal of this risk assessment is to define and determine the risks associated with cloud computing and how the risk factor can be related to other service level agreement factors such as the response time and the service cost. This helps to understand the risks associated with clouds and provide information for decision makers to decide wither to move to cloud or not. This task aims to analyze different critical areas in cloud so the cloud customer can ensure and understand the cloud risks associated with other SLA factors such as the response time and cost. This also helps the cloud customers to understand the surrounding issues with cloud so they can place security controls to resolve these risks concerns. The main strategy of this task is to measure the risk associated with the VMs in the cloud. First of all, this study calculates the risk associated with one VM. Then, it creates new VM and calculates the associated risk with the two VMs until to the last VM is created. In this task, the total number of VMs that the study creates is 10 VMs. The scope of this risk analysis is to determine the risks introduced while moving to cloud and creating up to 10 VMs.

4.3.2. Implementation (Do)

The implementation part contains the following processes: risk analysis, risk assessment, and risk mitigation. Each process of this step is done separately as the following:

4.3.2.1. Risk analysis

For this part, this research uses the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method as a general guide to perform the task. Since this method is being used in large-scale organization processes [29], some parts of this method are ignored in this study. This part tends to evaluate and identify the scenario assets, critical threats, and possible vulnerabilities. In addition to the OCTAVE method, this research also uses the Cloud Security Alliance guide to complete this task [12].

Risk analysis task contains the following processes:

4.3.2.1.1. Assets Identification and Evaluation

This research uses OCTAVE and Cloud Security Alliance (CSA) guide to identify the main assets that are reliable to this study scenario. The first OCTAVE step is to build assets-based threat profiles by identifying the important assets. Then, this research evaluates those assets to find the possible value of each asset. In term of the study scenario, it identifies the assets that are important to this scenario and to the cloud providers. In general, CSA declares that assets in cloud environments fall into two categories: data or application, functions, and processes. In the study scenario, information and functions are moved to cloud providers. Thus, this research uses the CSA guide to divide the assets to two different categories as the following [12]:

4.3.2.1.1.1. **Data**

Data is considered is one of the main assets in cloud environments since in this case, all the data has been moved to the cloud and there is no physical governance over the data anymore. This research recognizes the data that is resided in the VMs is sensitive data. There are different questions that need to be asked to

assess the confidentiality, integrity, and availability of the data. NIST defines confidentiality as "the security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit", integrity as "the security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation)" and availability as "the security goal that generates the requirement for protection against— • Intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data • Unauthorized use of system resources" [26]. Next, this research examines each one of these requirements using various questions provided by the CSA guide [12]:

- **Confidentiality**:

How would we be harmed if the data became widely public and widely distributed?

For this study scenario, the data is set to be private and it's only accessible by authorized user. The VMs need credentials to access the data that resides in the cloud since there is no data is set to be public. If any data breaches happen or the data has accessed by unintended users, the risk affecting the data confidentiality increases dramatically. This would cause real harm to the data.

How would we be harmed if an employee of the cloud provider accessed the data?

As the data is set to be private, this research needs to ensure that no one can access the data including the cloud provider unless the provider gets the permission. Thus, if the cloud provider accesses the data without permission, this would cause harmful risk to the data privacy. Also, this research needs to ensure the provider placed security controls to protect the data privacy.

- **Integrity:**

How would we be harmed if the information/data were unexpectedly changed?

The accuracy of the data should be assured to protect the authenticity of the data. Unexpected change may introduce risk if there is no backup process in place. Any unintended change to the data can

affect the data integrity and introduce more risks to the cloud. Indeed, this would harm the trust relationship between the cloud provider and the customer.

- **Availability:**

How would we be harmed if the data were unavailable for a period of time?

The data should be available as needed at any time. Any unavailability issue may cause negative impact on the data and the scenario. This research should ensure how Amazons manages the data availability and how the remote connection can affect the data availability.

4.3.2.1.1.2. Application, functions, and processes (virtual resources)

In this category, this research states that the vertical machines (VMs) in this scenario are the main assets for this study. Thus, this research assesses the security requirements against this asset as the following:

- **Confidentiality**:

How would we be harmed if the VMs became widely public and widely distributed?

For this scenario, this research sets up the VMs in a virtual private cloud in Amazon AWS. The VMs should be accessible by the authorized user only. If the VMs appear in the amazon public cloud, a risk is introduced and it may affect the VMs confidentiality.

How would we be harmed if an employee of the cloud provider accessed the VMs?

The VMs should be accessible by the authorized user only. Any unauthorized access to the VMs can cause harmful impact to the VMs confidentiality. This research needs to ensure that Amazon places good access controls that protect the VMs access.

- **Integrity:**

How would we be harmed if an outsider manipulated a process or a function in the VMs?

Authorized user is the only one who can manipulate any process in the VMs. Any unauthorized attempt to create, alter, or delete any process in the VMs would harm the VMs integrity. This research should ensure that the only ones who can control the VMs' processes, functions, and resources are the authorized people.

- **Availability:**

How would we be harmed if the VMs were unavailable for a period of time?

All VMs should be up available to us as needed. Any down time to the VMs may introduce high risks and affect the availability requirement. Thus, this research should ensure that Amazon could meet the uptime requirements stated in its SLA. All cloud resources that provide access function to the VMs should available all the time. These resources include internal networks, and virtual private cloud resources such as IPs, security groups, and subnets.

From the asset identification and evaluation task, this study concludes that the main assets that are very important in this study's scenario are the data and the VMs. Thus, this study uses a cloud deployment model that suits and meets this study's security requirements. This chosen model is the external private cloud in a shared infrastructure i.e. Amazon cloud services. Table 6 shows the assets classification and their impacts when a violation happens:

Assets	Data classification	Impact classification
Amazon EC2 Instances (VMs)	Private	High
Data resides in each VM	Private	Medium

Table 6: Assets classification

4.3.2.1.2. Threat Identification

NIST defines a threat as "the potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability" [26]. Additionally, NIST states that a threat source "either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability" [26]. In this part, the research uses different sources that help us to provide combined list of different threats that are related to the study's scenario. CSA provide a list of the top threats to cloud computing [30]. Also, Whitman provides a general list of threats to information security [31]. Table 7 contains different threats attached with the possible threat source and the motivation.

Some cloud-specific threats provided by the Cloud Security Alliance [30]	
Threat	Malicious Insiders
Threat source	• Inside adversaries. • Cloud provider employees. • Attackers
Motivation	• Data disclosure or destruction • Unauthorized data manipulation. • Money gain.
Critical Area	• Governance and Enterprise Risk Management
Threat	Shared Technology Issues
Threat source	• Attackers • Cloud customers • Lack of patching support from cloud provider.
Motivation	• Impact on other cloud customers' operation • Unauthorized activity. • Denial of service. • Unauthorized access.
Critical Area	• Virtualization
Threat	Data Loss or Leakage
Threat source	• Attackers. • Insiders.

	• Untrained cloud customers. • Weak encryption and key management by cloud provider.
Motivation	• Data disclosure. • Data manipulation or deletion. • Money gain. • Challenge
Critical Area	• Encryption and Key Management • Information Management and Data Security
Threat	Account or Service Hijacking
Threat source	• Attackers. • Weak authentication controls. • Weak monitoring techniques. • Lack of understanding the cloud provider policies.
Motivation	• Leverage the reputation of the cloud customer. • Use the attacked services to launch new attacks. • Compromise the availability of the service. • Compromise the integrity of the account.
Critical Area	• Governance and Enterprise Risk Management
Threat	Unknown Risk Profile
Threat source	• Cloud provider governance • Using unsecure systems, codes, software, or hardware. • Compliance issues in the internal security controls.

Motivation	• Exploit unknown vulnerabilities. • Launch unauthorized activity. • Impersonate cloud customers to gain trust from cloud provider.
Critical Area	• Governance and Enterprise Risk Management
Some general threats to information security [31]	
Threat	Deliberate Software Attacks
Threat source	• Viruses, worms, or malwares. • Vulnerable software, code, or system. • Weak patching management.
Motivation	• Exploit known vulnerabilities. • Denial of service • Leverage the reputation of the cloud customers. • Launch new attacks using gain services.
Critical Area	• Governance and Enterprise Risk Management • Virtualization
Threat	Act of Human Error or Failure
Threat source	• Cloud customers • Insiders
Motivation	• There is no motivation since the employee does unintentional error.
Critical Area	Governance and Enterprise Risk Management

Threat	QoS Deviations from Service Providers
Threat source	• Cloud/service provider
Motivation	• There is no motivation since the employee should try to provide high quality service.
Critical Area	Governance and Enterprise Risk Management

Table 7: Cloud-Specific Threats

4.3.2.1.3. Vulnerability Identification

NIST defines the vulnerability as "A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy" [26]. This part is very essential in risk assessment to identify the known vulnerabilities to protect the data and VMs from attacks caused by known vulnerabilities. Grobauer defines the vulnerability as "the probability that an asset will be unable to resist the action of a threat agent" [32]. In this task, this research determines and identifies cloud-specific vulnerabilities that could affect any cloud environment. Grobauer provides a list of cloud-specific vulnerabilities that this study uses in the analysis [32]. Bamiah and Brohi also provide a list of cloud-specific vulnerabilities that is used in the analysis too [33].

Cloud-specific vulnerabilities by Grobayer [32]	
Vulnerability	Vulnerable VM images provided by the cloud provider
Threat source	Cloud/service providers
Threat action	The cloud customer launches new VM using a pre-defined vulnerable VM image.
Critical area	Governance and Enterprise Risk Management
Vulnerability	Collect detailed information about configuration, patch management, and code.

Threat source	Attackers
Threat action	The attacker rents a VM and uses its administrative features to collect important information such as cloud infrastructure, patch management, and API code.
Critical area	• Information Management and Data Security • Governance and Enterprise Risk Management
Vulnerability	Vulnerable VM images distributed in a virtual images store
Threat source	Cloud customer
Threat action	The cloud customer uses untrusted and vulnerable VM image that is available in VM images store.
Critical area	Governance and Enterprise Risk Management
Vulnerability	Data leakage while cloning the VM
Threat source	Cloud provider
Threat action	When a provider clones a VM, data leakage happens during the cloning since this process copies data and private key for a host. Then, all the data in this VM go public when a VM launches using the cloned image.
Critical area	Information Management and Data Security
Vulnerability	Weak random key generation and weak key management.
Threat source	Cloud provider
Threat action	Virtualization may introduce a problem between the hardware and OS kernel, which leads to weak random key

	generation
Critical area	• Encryption and Key Management • Virtualization
Vulnerability	Data recovery vulnerability
Threat source	Cloud provider
Threat action	This happens when a provider faces a problem in backing up the VMs and this leads to VM loss.
Critical area	Information Management and Data Security
Vulnerability	Data destruction policies
Threat source	Cloud provider
Threat action	When a customer does not need the cloud service anymore, the provider should remove all his data from the virtual storage only. The provider can't wipe the physical disk if it is still used by other shared users.
Critical area	• Governance and Enterprise Risk Management • Information Management and Data Security
Cloud-specific vulnerabilities by Bamiah and Brohi [33]	
Vulnerability	Virtual Machine Escape
Threat source	Attacker
Threat action	There is more risk when the VM OS is same as cloud host OS since they might share the same vulnerability. Also, co-location of VMs in a shared host increases the attack surface. Finally, the attacker can use his VM to attack and

	compromise the host.
Critical area	Governance and Enterprise Risk Management
Vulnerability	Insecure Cryptography
Threat source	• Cloud provider • Attacker
Threat action	When cloud provider uses the virtualization to partition a physical server to multiple VMs, this server may generate weak random key due to the lack of sufficient entropy pool. Thus, creating truly random key in cloud environment is much harder than a detected PC desktop. This may allow the attacker to decode cryptographic text easily.
Critical area	• Encryption and Key Management • Information Management and Data Security • Virtualization
Vulnerability	Internet Dependency
Threat source	Cloud provider
Threat action	Most of the cloud services depend totally on the Internet so the user can reach and utilize those services. Any Internet issue increases the risk of service availability since the service is useless if it's unavailable.
Critical area	Governance and Enterprise Risk Management

Table 8: Cloud-Specific Vulnerabilities

4.3.2.2. Risk assessment

NIST states that risk assessment is "the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact" [26]. According to this framework [8], this part is divided into three different steps:

4.3.2.2.1. Likelihood Determination (L)

NIST states that the likelihood determination aims "to derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment" [26]. This step tends to estimate the likelihood of a vulnerability to be exploited or occurred. This part also uses the results from the vulnerability identification step in section 4.3.2.1.3. The vulnerability is evaluated and assigned a numeric value and likelihood level. The numeric value ranges from 0.1 to 1.0. A value of 0.1 means the probability of a vulnerability being exploited is very low while a value of 1.0 means the probability of a vulnerability being exploited is very high. The vulnerability likelihood levels are high, medium, and low. Similarly, high level means the threat source has high motivations or capabilities to exploit certain vulnerability while low level indicates the lack of required skills and incentives to exploit given vulnerability. The following table identifies each vulnerability and its likelihood level and rate.

Likelihood Estimation			
Vulnerability	**Affected Assets**	**Likelihood Level**	**Likelihood rate**
Vulnerable VM images provided by the cloud provider.	Amazon VMs	Medium	0.5
Collecting detailed information about configuration, patch management, and code.	Amazon VMs	High	1.0
Vulnerable VM images distributed in	Amazon	Medium	0.5

a virtual images store	VMs		
Data leakage while cloning the VM	Data	Medium	0.5
Data destruction policies	Data	High	1.0
Data recovery vulnerability	Data	Low	0.1
Weak random key generation and weak key management.	Amazon VMs Data	Medium	0.5
Virtual machine escape	Amazon VMs	Low	0.1
Insecure cryptography	Data	Low	0.1
Internet dependency	Amazon VMs	Low	0.2

Table 9: Likelihood identification

Next, this research needs to identify the likelihood of exploiting vulnerabilities on certain cloud assets. This research uses the next formula to achieve this goal:

Likelihood of exploiting vulnerabilities on assets= total likelihood rate of an asset / the number of caused vulnerabilities

Likelihood of exploiting vulnerabilities on (Amazon EC2 VMs) =

(0.5 + 1.0 + 0.5 + 0.5 + 0.1 + 0.1) / 6 = 2.7 / 6 = 0.45

Likelihood of exploiting vulnerabilities on (data) =

(0.5 + 1.0 + 0.1 + 0.5 + 0.2) / 5 = 2.3 / 5 = 0.46

4.3.2.2.2. Impact analysis (I)

NIST states that impact analysis task aims "to determine the adverse impact resulting from a successful threat exercise of vulnerability" [26]. In this step, this study assesses the loss impact of each asset based on its value. The impact level is divided into three levels: high, medium, and low where high

level represents high value asset that may cause high impact to the study's scenario while low impact level states the least value assets in the scenario. Each asset is given impact rete that ranges from 1 to 100:

Impact Estimation			
Threat	**Affected Assets**	**Impact Level**	**Impact rate**
Malicious Insiders	Amazon VMs	High	100
Shared Technology Issues	Amazon VMs and data	High	90
Data Loss or Leakage	Data	Medium	60
Account or Service Hijacking	Amazon VMs, data	High	80
Deliberate Software Attacks	Amazon VMs	High	80
Act of Human Error or Failure	Amazon VMs	Low	20
QoS Deviations from Service Providers	Amazon VMs, data	Medium	50
Unknown Risk Profile	Amazon VMs, data	High	90

Table 10: Impact estimation

From Table 10, this research estimates the asset value based on how a threat impacts given assets. Then, it calculates the total value of each asset and finds the average as the following:

Impact value of an asset= total impact rate of an asset / the number of caused threats

Impact value of an Amazon EC2 VM =

(100 + 90 + 80 + 80 + 20 + 50 + 90) / 7 = 510 / 7 = 72.8

Impact value of data asset = (90 + 60 + 80 + 50 + 90) / 5 = 370 / 5 = 74

4.3.2.2.3. Risk Determination (R)

After this study determines vulnerabilities likelihoods, and the threats impacts, it uses the outputs to evaluate and determine the risk level of each asset. NIST declares, "The purpose of this step is to assess the level of risk to the IT system" [26]. To calculate the risk factor, this research uses the following formula:

Risk (R) = (Likelihood (L) x Impact (I)) - (percentage of risk mitigated by current controls of given Vulnerability (%CC) x Likelihood (L) x Impact (I)) + (Uncertainty of given Vulnerability (U) x Likelihood (L) x Impact (I))

This formula is adapted from this original formula [34]:

Risk = Likelihood of vulnerability x impact – percentage risk already controlled + element of uncertainly

This formula has four variables:

Likelihood (L):

Likelihood of exploiting vulnerabilities on (Amazon EC2 VMs) = 0.45

Likelihood of exploiting vulnerabilities on (data) = 0.44

Impact (I):

Impact value of an Amazon EC2 VM= 72.8

Impact value of data asset = 74

Percentage of risk mitigated by current controls (CC):

This variable states the current controls that are placed to mitigate risks that impact the assets. In this study's scenario, this research estimates the value based on what Amazon has developed to protect the cloud assets.

Uncertainty (U):

Since it is not possible in risk management to know exactly everything about vulnerabilities, threats, and attacks or how the current controls are placed to reduce or mitigate the risks, the uncertainty variable is

used to substitute the unknown errors in the estimations. If the data is 80% accurate, the uncertainty factor is 100 – 80 = 20%.

Next are calculation tables of risk factor for the vulnerabilities:

Vulnerability #1: Vulnerable VM images provided by the cloud provider.

Asset	# VM	Impact (I)	Likelihood rate (L)	Uncertainty %	Current Controls %	Risk Factor (R_i) %	$\sum_1^i Risk\ Factor$ %
VMs	1	72.8	0.5	5%	98%	(72.8 x 0.5) – ((72.8 x 0.5) x 0.98) + ((72.8 x 0.5) x 0.05) = 2.548/100 = 0.02548	R= 1-(1-R_1)= 1-(1- 0.02548) = 0.02548
VMs	2	72.8	0.5	5%	98%	0.02548	R=1-(1-R_1)(1-R_2) = 1-(1-0.02548)(1-0.02548) = 0.0503107696
VMs	3	72.8	0.5	5%	98%	0.02548	0.07450885119
VMs	4	72.8	0.5	5%	98%	0.02548	0.09809036566
VMs	5	72.8	0.5	5%	98%	0.02548	0.12107102314
VMs	6	72.8	0.5	5%	98%	0.02548	0.14346613347
VMs	7	72.8	0.5	5%	98%	0.02548	0.16529061639
VMs	8	72.8	0.5	5%	98%	0.02548	0.18655901148
VMs	9	72.8	0.5	5%	98%	0.02548	0.20728548787
VMs	10	72.8	0.5	5%	98%	0.02548	0.22748385364

Table 11: Risk factor for vulnerability#1

To estimate the current controls in Table 11, this study searched for different issues that have happened in Amazon AWS. These issues are related to pre-define images that Amazon provides in its store and the community store. For instance, Amazon reported that certain Linux images have a common vulnerability [35]. Also, Amazon reported that certain public EC2 AMIs have Linux 2.6 kernel vulnerability [35]. Eric Hammond states in Amazon forums that Amazon has weakness in generating SSH host key where the old AMIs bundle the same SSH host key [36]. This means that each instance launches from that public AMI will the same SSH host key and anyone can access any instance used that public AMI. Then, Amazon solved this issue and forced that the public AMI should generate unique SSH host key for each new launched instance [37]. All these issues indicate that there are always some issues with the public AMIs provided by Amazon. Some of them have been resolved while there might be some hidden issues. From the provided resources, Amazon provided better controls whenever a Linux issue appeared while leaving most of the windows issues to the Microsoft updates. All current controls percentages and uncertainty factors would reflect those issues.

It is appeared that the vulnerable images are considered as possible of risk. Figure 10 shows the risk factor for this vulnerability goes up gradually while increasing the number of used VMs. Thus, adding more VMs can increase the risk of this vulnerability by using vulnerable images.

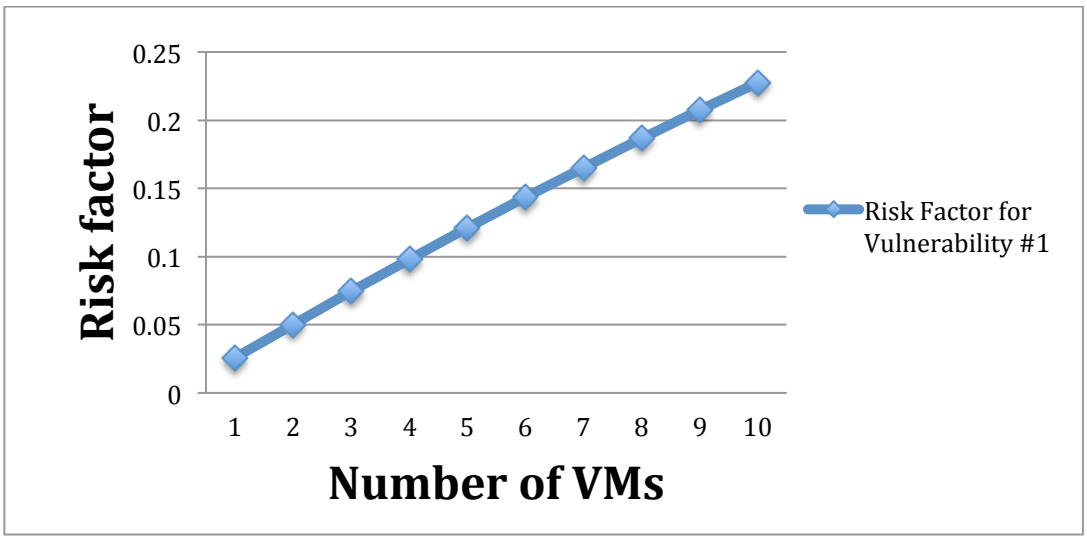

Figure 10: Risk factor for vulnerability#1

Vulnerability #2: Collecting detailed information about configuration, patch management, and code.

Asset	# VM	Impact (I)	Likelihood rate (L)	Uncertainty %	Current Controls %	Risk Factor (R_i) %	$\sum_1^i$ *Risk Factor* %
VMs	1	72.8	1.0	3%	85%	(72.8 x 1.0) – ((72.8 x 1.0) x 0.85) + ((72.8 x 1.0) x 0.03) = 13.104/100 = 0.13104	1-(1- 0.13104) = 0.13104
VMs	2	72.8	1.0	3%	85%	0.13104	0.2449085184
VMs	3	72.8	1.0	3%	85%	0.13104	0.34385570614
VMs	4	72.8	1.0	3%	85%	0.13104	0.42983685441
VMs	5	72.8	1.0	3%	85%	0.13104	0.50455103301
VMs	6	72.8	1.0	3%	85%	0.13104	0.56947466564
VMs	7	72.8	1.0	3%	85%	0.13104	0.62589070546

VMs	8	72.8	1.0	3%	85%	0.13104	0.67491398741
VMs	9	72.8	1.0	3%	85%	0.13104	0.7175132585
VMs	10	72.8	1.0	3%	85%	0.13104	0.75453032111

Table 12: Risk factor for vulnerability#2

For vulnerability #2 in Table 12, any attacker has various opportunities to collect as much information as he/she can about the Amazon AWS. Amazon provides very detailed documents about how to use and manage all its cloud services and APIs. The attacker can use those documents to understand how Amazon services works. Also, the attacker can register and use the services as regular user, then, he can get insight view how an instance is being configured and what the default settings and minimum-security controls are. All these rich information can help the attacker to find good strategies to attack any service hosted by Amazon services. Thus, it is clear that an attacker can easily use this vulnerability, which leads to 3% of uncertainty.

Collecting information about the cloud infrastructure can be an easy task for an attacker due to the many options that he/she can use to complete the task. In the analysis, Figure 11 demonstrates that risk factor of collection information from cloud environments keeps growing steadily while adding the VMs one after the other. For this vulnerability, the risk factor ranges from 0.13104 for one VM to 0.75453 for 10 VMs.

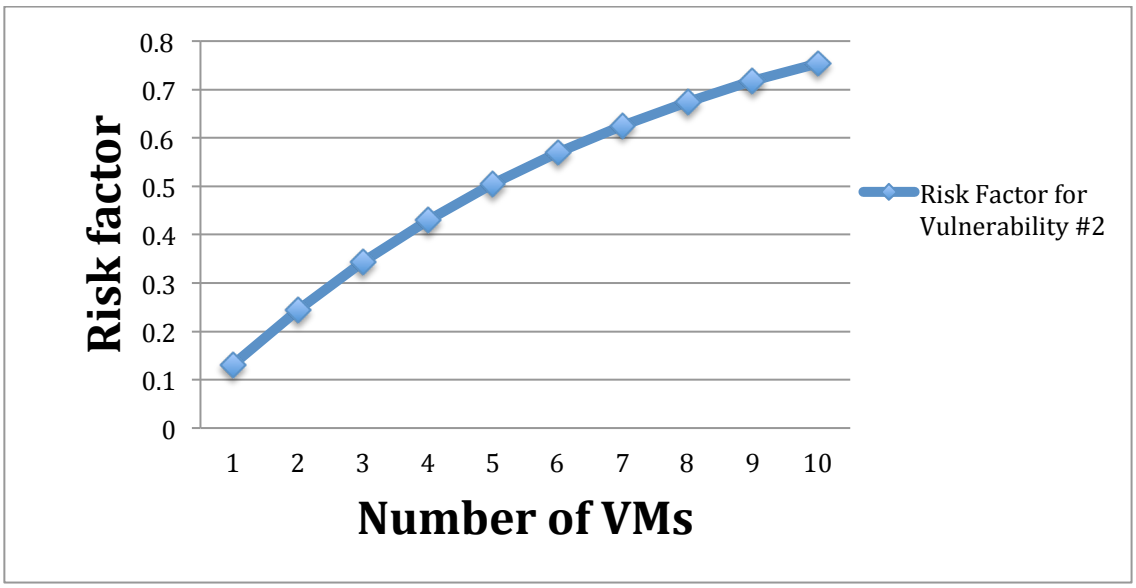

Figure 11: Risk factor for vulnerability#2

Vulnerability #3: Vulnerable VM images distributed in a virtual images store.

Asset	# VM	Impact (I)	Likelihood rate (L)	Uncertainty %	Current Controls %	Risk Factor (R_i) %	$\sum_1^i$ *Risk Factor* %
VMs	1	72.8	0.5	5%	95%	3.64/100 = 0.0364	1-(1 – 0.0364) =0.0364
VMs	2	72.8	0.5	20%	80%	0.0364	0.07147504
VMs	3	72.8	0.5	20%	80%	0.0364	0.10527334854
VMs	4	72.8	0.5	30%	60%	0.0364	0.13784139865
VMs	5	72.8	0.5	20%	80%	0.0364	0.169223972
VMs	6	72.8	0.5	30%	60%	0.0364	0.199464219
VMs	7	72.8	0.5	20%	80%	0.0364	0.228603722
VMs	8	72.8	0.5	30%	60%	0.0364	0.256682546
VMs	9	72.8	0.5	30%	60%	0.0364	0.283739301

VMs	10	72.8	0.5	30%	60%	0.0364	0.309811191

Table 13: Risk factor for vulnerability #3

In Table 13, this vulnerability is almost the same as vulnerability #1 since Amazon provides community store for public AMIs where any user can bundle a given instance and build an AMI. Then, the user can place this AMI in the community AMIs store so any user can use that AMI. It is clear that there is a chance that one of the published AMI might be vulnerable. Thus, in Table 13, the same estimations in Table 11 are used.

Using VM images from public or community store introduce more risk to the cloud environments. Similar to Figure 10, Figure 12 depicts that the risk factor of this vulnerability increasingly accumulates from a factor of 0.0364 per one VM to a total of 0.3098 for all the VMs.

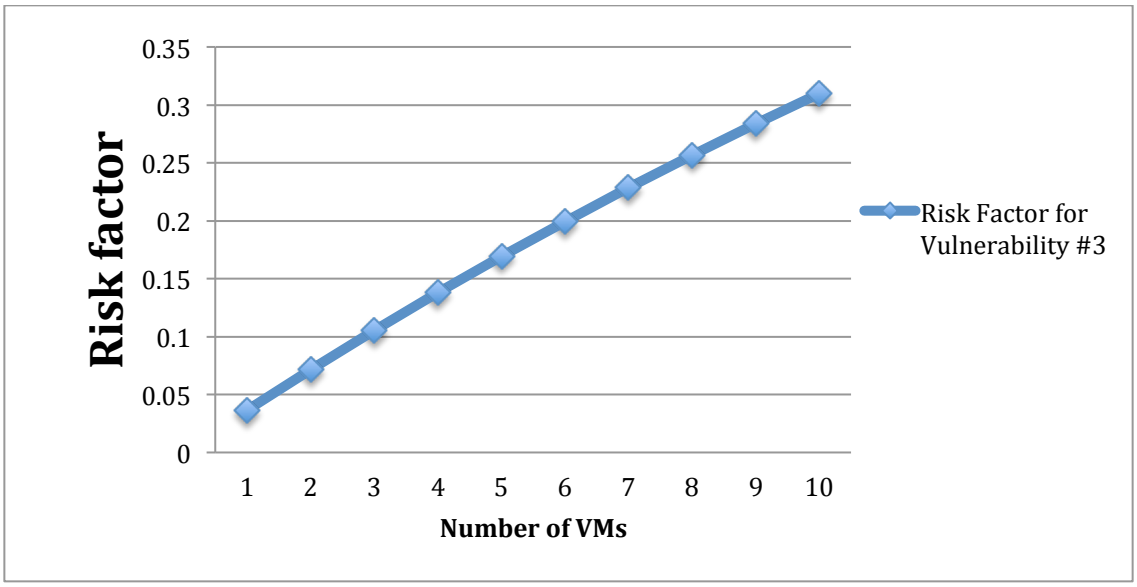

Figure 12: Risk factor for vulnerability #3

Vulnerability #4: Data leakage while cloning the VM

Asset	# VM	Impact (I)	Likelihood rate (L)	Uncertainty %	Current Controls %	$\sum_1^i$ *Risk Factor* %	$\sum_1^i$ *Risk Factor* %
Data	1	74	0.5	10%	97%	(74 x 0.5) – ((74 x 0.5) x 0.97) + ((74 x 0.5) x 0.1) = 4.81/100 =0.0481	1-(1-0.0481) = 0.0481
Data	2	74	0.5	10%	97%	0.0481	0.09388639
Data	3	74	0.5	10%	97%	0.0481	0.137470455
Data	4	74	0.5	10%	97%	0.0481	0.178958126
Data	5	74	0.5	10%	97%	0.0481	0.21845024
Data	6	74	0.5	10%	97%	0.0481	0.256042783
Data	7	74	0.5	10%	97%	0.0481	0.291827126
Data	8	74	0.5	10%	97%	0.0481	0.325890241
Data	9	74	0.5	10%	97%	0.0481	0.35831492
Data	10	74	0.5	10%	97%	0.0481	0.389179973

Table 14: Risk factor for vulnerability #4

In Vulnerability #1, this study states that Amazon had an issue while cloning an instance to build an AMI. The private SSH host key would be leaked and copied to the new AMI, which leads to enormous privacy issues [36]. After Amazon solved this issue, this study could estimate that Amazon provided better controls for the cloning process as appeared in Table 14.

Data leakage is one of the issues that forces decision makers to not move to cloud. Cloning process one of the main features of the cloud environments, which help to backup exiting environment or provides an elastic environment. As a result of the analysis, Figure 13 shows that risk factor of data leakage in cloning process goes up gradually as the number of the number of VMs increases. The risk factor increases from a value of 0.0481 to a total of 0.3891.

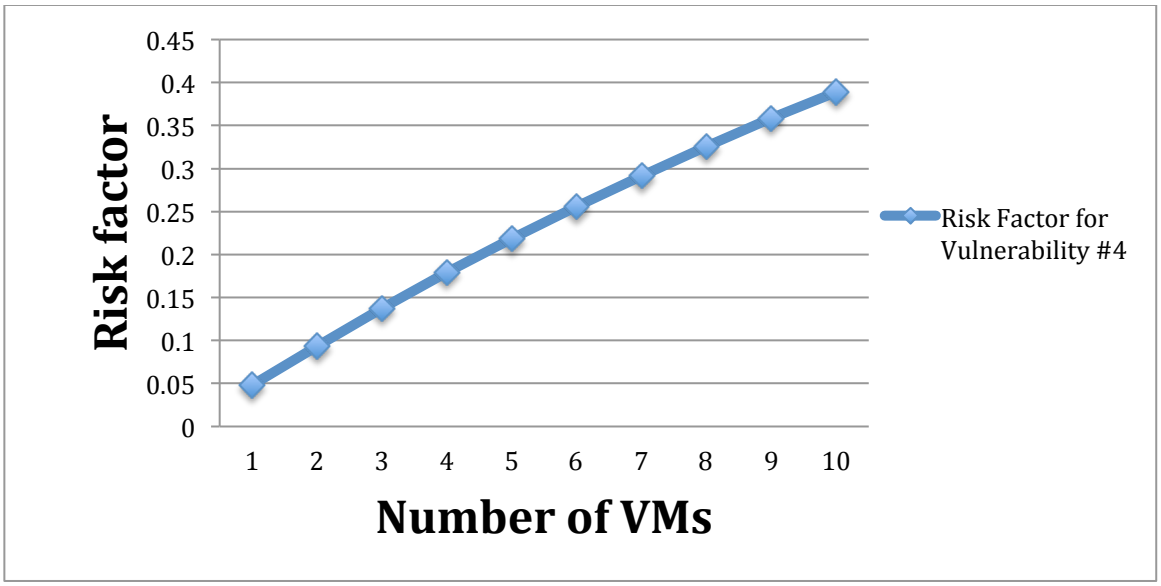

Figure 13: Risk factor for vulnerability #4

Vulnerability #5: Data destruction policies

Asset	# VM	Impact (I)	Likelihood rate (L)	Uncertainty %	Current Controls %	$\sum_1^i$ *Risk Factor* %	$\sum_1^i$ *Risk Factor* %
Data	1	74	1.0	15%	90%	(74 x 1.0) – ((74 x 1.0) x 0.90) + ((74 x 1.0) x 0.15) = 18.5/100 = 0.1850	0.1850
Data	2	74	1.0	15%	90%	0.1850	0.335775

Data	3	74	1.0	15%	90%	0.1850	0.458656625
Data	4	74	1.0	15%	90%	0.1850	0.558805149
Data	5	74	1.0	15%	90%	0.1850	0.640426197
Data	6	74	1.0	15%	90%	0.1850	0.70694735
Data	7	74	1.0	15%	90%	0.1850	0.761162091
Data	8	74	1.0	15%	90%	0.1850	0.805347104
Data	9	74	1.0	15%	90%	0.1850	0.84135789
Data	10	74	1.0	15%	90%	0.1850	0.87070668

Table 15: Risk factor for vulnerability #5

Amazon does not state clearly its procedures for data destruction in Amazon EC2 instances. Amazon states that users who require data to be wiped have the responsibility to use special method to wipe Amazon Elastic Block Storage (EBS) devices [38]. The EBS devices are the only storage devices that can be wiped by the customer. In Amazon S3, for instance, if a customer wants to delete data, Amazon just removes the mapping between the customer and data object. Amazon does not declare how it deletes and wipes customer data from the shared storage. This leads to a chance where the data can be restored from the physical storage. On the other hand, Amazon states that if a storage device is not used anymore, Amazon has a decommissioning process to destroy the data and this process may include physical destruction for the storage device if needed [38]. In Table 15, the uncertainly and current controls are estimated based on what information in Amazon security reports [38] [28].

Data destruction in cloud environments is ambiguous process since the data is stored in shared storage. Thus, the physical storage devices cannot be wiped completely. As a result, the analysis results in Figure 14 indicate the risk factor of data destruction increases significantly when the test cloud uses more VMs since adding more VMs results in more data that need to be destroyed at some point. The risk factor rises from 0.1850 of one VM to 0.8707 of 10 VMs.

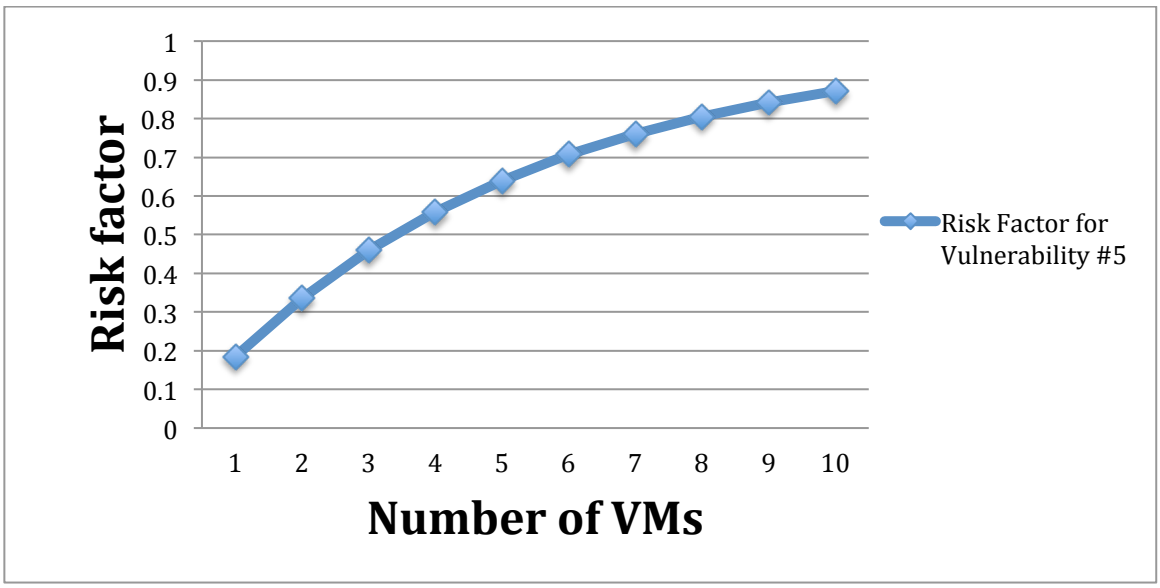

Figure 14: Risk factor for vulnerability #5

Vulnerability #6: Data recovery vulnerability

Asset	# VM	Impact (I)	Likelihood rate (L)	Uncertainty %	Current Controls %	$\sum_1^i$ *Risk Factor* %	$\sum_1^i$ *Risk Factor* %
Data	1	74	0.1	10%	95%	(74 x 0.1) – ((74 x 0.1) x 0.95) + ((74 x 0.1) x 0.1) = 1.11/100 =0.111	0.111
Data	2	74	0.1	10%	95%	0.111	0.209679
Data	3	74	0.1	10%	95%	0.111	0.297404631
Data	4	74	0.1	10%	95%	0.111	0.375392717
Data	5	74	0.1	10%	95%	0.111	0.444724125
Data	6	74	0.1	10%	95%	0.111	0.506359747

Data	7	74	0.1	10%	95%	0.111	0.561153815
Data	8	74	0.1	10%	95%	0.111	0.609865742
Data	9	74	0.1	10%	95%	0.111	0.653170645
Data	10	74	0.1	10%	95%	0.111	0.691668703

Table 16: Risk factor for vulnerability #6

For data recovery, Amazon states that it stores all the data of the Amazon services in multiple locations to provide a better backup process [38]. Amazon stores the data in multiple availability zones in different physical locations while it stores redundant backups for the Amazon EBS in the same availability zone. Also, Amazon dose not backup any virtual disk attached to a running instance. Nevertheless, Amazon experienced severe crash that affects its EC2 cloud services and lead to permanently data loss [39]. It is appeared that some data of many customers have lost and cannot be recovered even though Amazon claims it has good recovery process that has been tested extensively. In Table 16, the values are estimated based on what Amazon claims and what issues have occurred in the Amazon services so far.

Figure 15 demonstrates the importance of data recovery risk on data security. It is clear from the chart that the risk factor of the data recovery keeps increasing while the number of the VMs increases. This shows that adding more VMs results in higher data recovery risk. The risk factor has increased from a value of 0.111 to a total of 0.6916.

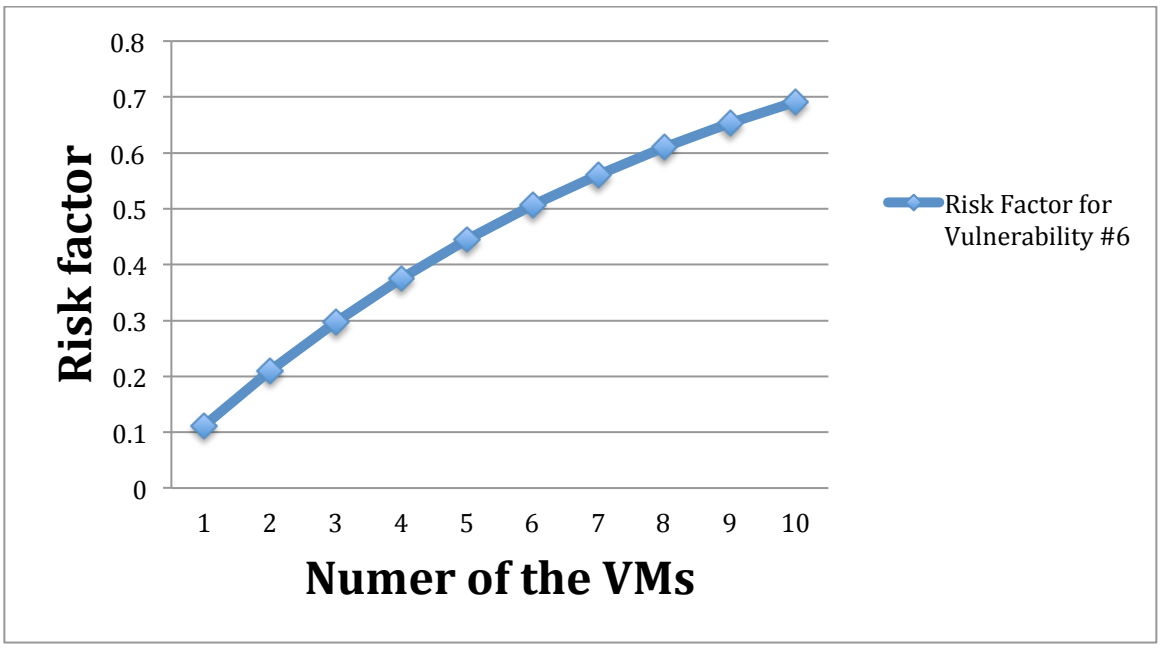

Figure 15: Risk factor for vulnerability #6

Vulnerability #7: Weak random key generation and weak key management.

Asset	# VM	Impact (I)	Likelihood rate (L)	Uncertainty %	Current Controls %	$\sum_1^i$ *Risk Factor* %	$\sum_1^i$ *Risk Factor* %
VMs Data	1	(74+ 72.8) / 2 =73. 4	0.5	30%	95%	(73.4 x 0.5) – ((73.4 x 0.5) x 0.95) + ((73.4 x 0.5) x 0.3) = 12.845/100 0.12845	0.12845
VMs Data	2	73.4	0.5	30%	95%	0.12845	0.240400598
VMs Data	3	73.4	0.5	30%	95%	0.12845	0.337971141
VMs	4	73.4	0.5	30%	95%	0.12845	0.423008748

Data							
VMs Data	5	73.4	0.5	30%	95%	0.12845	0.497123274
VMs Data	6	73.4	0.5	30%	95%	0.12845	0.56171779
VMs Data	7	73.4	0.5	30%	95%	0.12845	0.618015139
VMs Data	8	73.4	0.5	30%	95%	0.12845	0.667081095
VMs Data	9	73.4	0.5	30%	95%	0.12845	0.709844528
VMs Data	10	73.4	0.5	30%	95%	0.12845	0.747114999

Table 17: Risk factor for vulnerability #7

Amazon uses different security credentials that allow customer to interact with the cloud services such as AWS access key, X.509 certificate, web-based app password, and virtual or hardware multi factor authentication (MFA) [38]. No serious issues have been reported about Amazon key management processes except security issues related with certain remote-based connection software such as Microsoft remote desktop [40]. In Table 17, the values are estimated based on current information provided by Amazon.

The process of generating managing the encryption keys is very critical in cloud environments. No reports have been issued concerning any issue with the amazon key generation and management, which reflects the estimations. Nevertheless, Figure 16 depicts the steady increase in the risk factor from 0.1284 for one VM to a total of 0.7471 for 10 VMs. This increase is justified when there is key management issue while adding more VMs. Thus, each VM is vulnerable to this vulnerability.

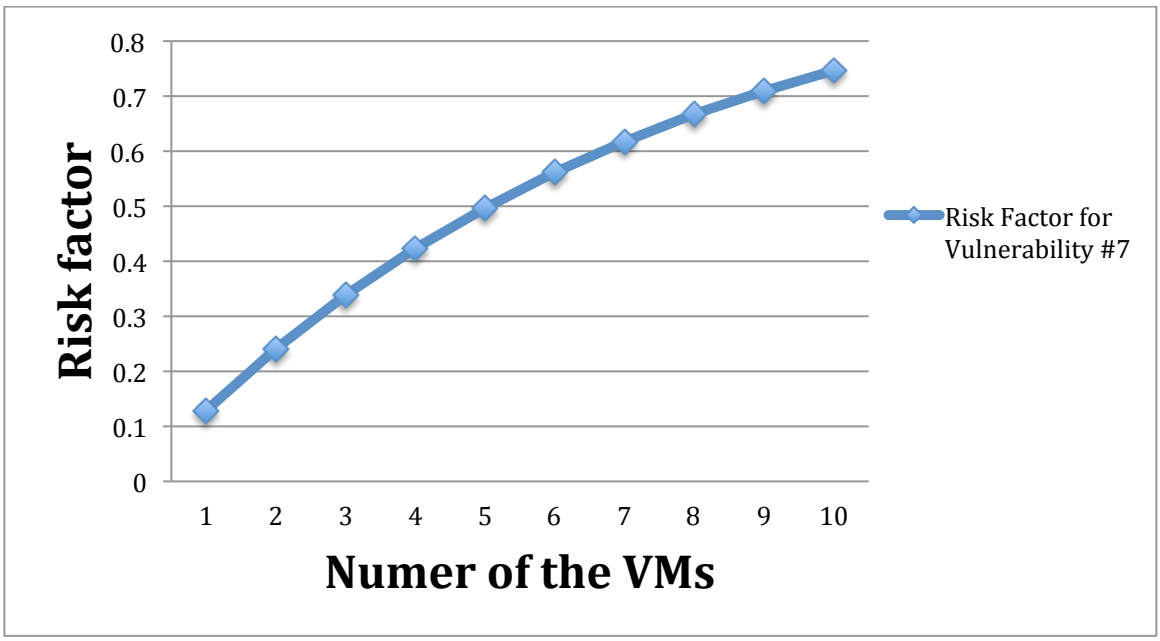

Figure 16: Risk factor for vulnerability #7

Vulnerability #8: Virtual machine escape

Asset	# VM	Impact (I)	Likelihood rate (L)	Uncertainty %	Current Controls %	$\sum_1^i$ *Risk Factor* %	$\sum_1^i$ *Risk Factor* %
VMs	1	72.8	0.1	10%	95%	(72.8 x 1.0) – ((72.8 x 1.0) x 0.95) + ((72.8 x 1.0) x 0.1) = 10.92/100 = 0.1092	0.1092
VMs	2	72.8	0.1	10%	95%	0.1092	0.20647536
VMs	3	72.8	0.1	10%	95%	0.1092	0.293128251
VMs	4	72.8	0.1	10%	95%	0.1092	0.370318646
VMs	5	72.8	0.1	10%	95%	0.1092	0.43907985
VMs	6	72.8	0.1	10%	95%	0.1092	0.50033233

VMs	7	72.8	0.1	10%	95%	0.1092	0.55489604
VMs	8	72.8	0.1	10%	95%	0.1092	0.603501392
VMs	9	72.8	0.1	10%	95%	0.1092	0.64679904
VMs	10	72.8	0.1	10%	95%	0.1092	0.685368585

Table 18: Risk factor for vulnerability #8

This vulnerability is most of time found in a hypervisor, which allows the attacker to access, all resources managed by the hypervisor. These resources include the VMs, shared network resources, and shared storage resources. Up to now, Amazon has announced no hypervisor vulnerability. Although, Amazon announced some security advisories related to vulnerabilities found in Xen [41] [42]. In both announcements, Amazon states that all issues have not affected AWS customers. In Table 18, the values are estimated based on amazon announcement and the chance of hypervisor vulnerabilities.

Figure 17 illustrates that the risk factor of the VM escape escalates gradually as while adding more VMs to the cloud environment. If this vulnerability occurs, it affects the available VMs so adding VMs leads to higher risk of this vulnerability. The risk factor increases from a value of 0.1092 to a total of 0.6853 for all the VMs.

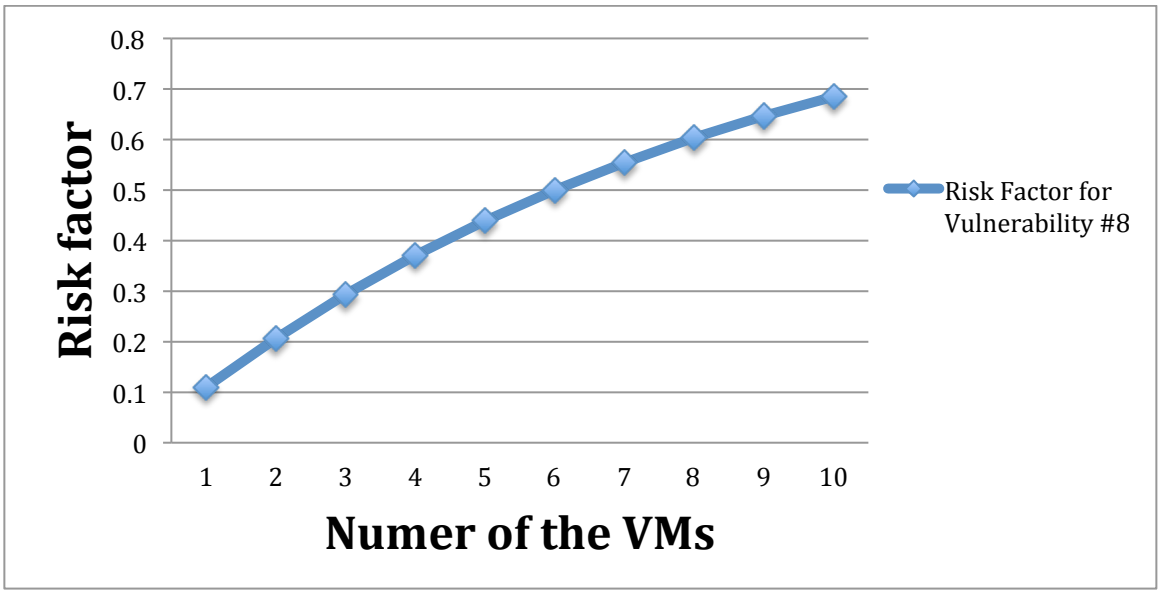

Figure 17: Risk factor for vulnerability #8

Vulnerability #9: Insecure cryptography

Asset	# VM	Impact (I)	Likelihood rate (L)	Uncertainty %	Current Controls %	$\sum_1^i$ *Risk Factor* %	$\sum_1^i$ *Risk Factor* %
Data	1	74	0.1	5%	95%	(74 x 0.1) − ((74 x 0.1) x 0.95) + ((74 x 0.1) x 0.05) = 0.74/100 =0.0074	0.0074
Data	2	74	0.1	5%	95%	0.0074	0.01474524
Data	3	74	0.1	5%	95%	0.0074	0.022036125
Data	4	74	0.1	5%	95%	0.0074	0.029273058
Data	5	74	0.1	5%	95%	0.0074	0.036456437
Data	6	74	0.1	5%	95%	0.0074	0.04358666
Data	7	74	0.1	5%	95%	0.0074	0.050664118
Data	8	74	0.1	5%	95%	0.0074	0.057689204
Data	9	74	0.1	5%	95%	0.0074	0.064662304
Data	10	74	0.1	5%	95%	0.0074	0.071583803

Table 19: Risk factor for vulnerability #9

In general, Amazon provides good security controls that allow customers to encrypt their information at rest. Amazon states that data storage such as Amazon S3 is only accessible through SSL endpoints, which protect data while in transition [38]. On the other hand, the data at rest is by default unencrypted and the customers has the option to encrypt the data using some method provided by Amazon such as Server Side Encryption (SSE) [43].

Insecure cryptography can be serious issue in any environment. In cloud environments, the vulnerability may have enormous impact on the cloud resources and it may result in many privacy and security issues. Thus, Figure 18 expresses the important behavior of the risk factor of this vulnerability. The risk factor increases substantially while using more cloud resources. Consequently, this vulnerability introduces a higher risk on the cloud environments. Its risk factor ranges from a value of 0.0074 for one VM to a total of 0.0715 for 10 VMs.

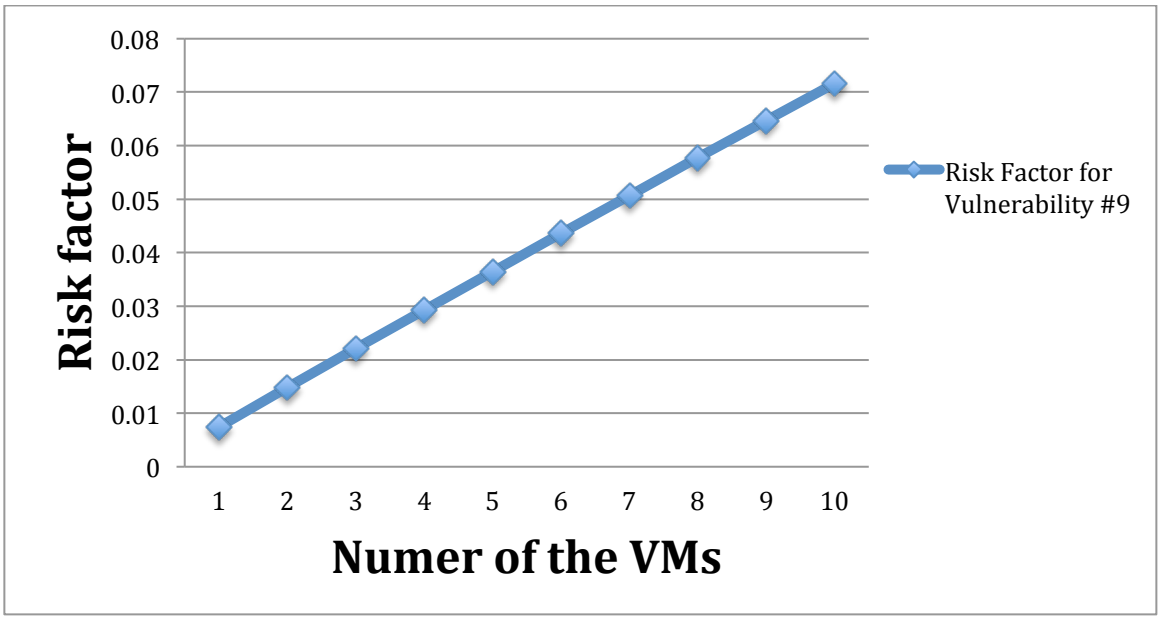

Figure 18: Risk factor for vulnerability #9

Vulnerability #10: Internet dependency

Asset	# VM	Impact (I)	Likelihood rate (L)	Uncertainty %	Current Controls %	$\sum_1^i$ *Risk Factor* %	$\sum_1^i$ *Risk Factor* %
VMs	1	72.8	0.2	10%	93%	(72.8 x 0.2) − ((72.8 x 0.2) x 0.93) + ((72.8 x 0.2) x 0.1) = 2.4752/ 100	0.024752

						=0.024752	
VMs	2	72.8	0.2	10%	93%	0.024752	0.048891338
VMs	3	72.8	0.2	10%	93%	0.024752	0.07243318
VMs	4	72.8	0.2	10%	93%	0.024752	0.095392314
VMs	5	72.8	0.2	10%	93%	0.024752	0.117783163
VMs	6	72.8	0.2	10%	93%	0.024752	0.139619795
VMs	7	72.8	0.2	10%	93%	0.024752	0.160915925
VMs	8	72.8	0.2	10%	93%	0.024752	0.181684934
VMs	9	72.8	0.1	10%	93%	0.024752	0.201939869
VMs	10	72.8	0.1	10%	93%	0.024752	0.221693453

Table 20: Risk factor for vulnerability #10

Amazon AWS customers relay completely on the Internet to use and interact with the Amazon cloud services. Any network disruptions severely affect the availability of the cloud resources. Amazon has faced different outages through the past years. In June 2012, an Amazon suffered an outage that impacted many businesses and large-scale companies that extremely relay on Amazon services such as Netflix, and Instagram and this outage was caused by a natural disaster [44]. Also, in Jun 2012, Amazon suffered another outage that affected many businesses such Pinterest and Dropbox [45]. In addition, many Amazon outages reported in news [46] [47]. Amazon states that all its data centers are online and no datacenter is set as a cold data center to ensure high availability and business continuity management [38]. Furthermore, Amazon claims that its systems are designed to tolerate any system or hardware failures with less impact. It provides automated processes to move traffic from any area that has a failure. Also, Amazon claims that it has good incident response and business continuity plans to be used whenever an incident happens. In its SLA, Amazon states that the annual uptime percentage is at least

99.95% per year [48]. In Table 20, the factors values are estimated based on the services outages and the current controls placed by Amazon.

Most of the cloud environments depend on the Internet to reach the cloud resources. If there is any connection disruption, this causes to an availability issue. This leads to massive impact on the cloud environments since all the cloud resources are useless at this point. Figure 19 represents this issue and how the risk factor rises while having more cloud resources. The increase risk of unavailability in cloud environments depend on the number of cloud resources. The risk factor increases from 0.02475 to 0.22169 for all VMs.

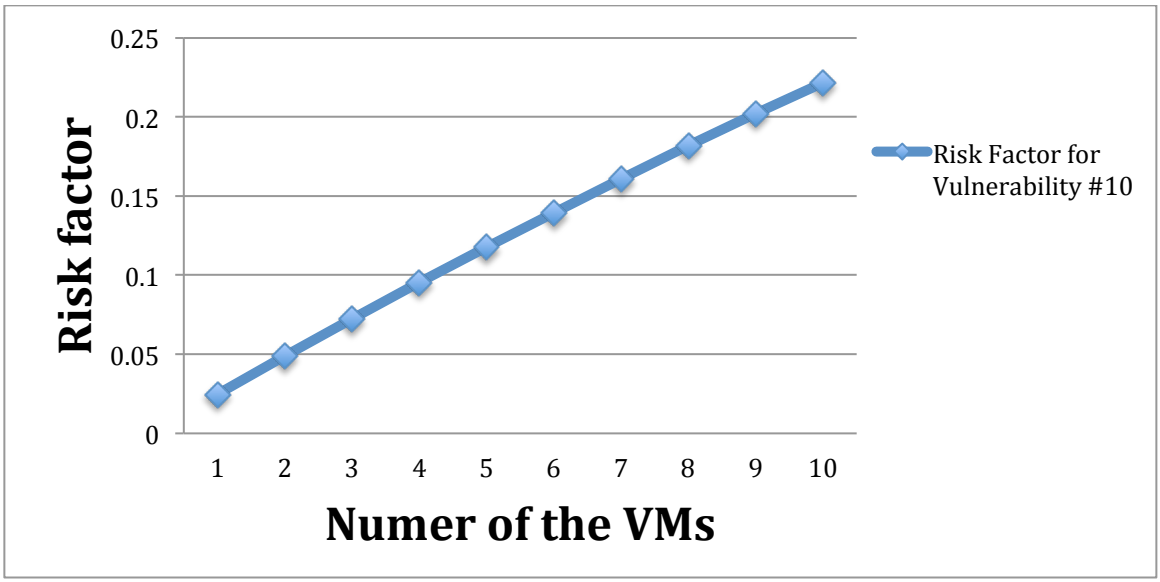

Figure 19: Risk factor for vulnerability #10

Figure 20 illustrates the overall behavior of the risk factor for all vulnerabilities while adding more VMs to the cloud environment. In general, the risk factor increases in all cases but the increase rate depends on the vulnerabilities. It is clear from the chart the increase rate for vulnerability #5 “Data destruction policies” is the highest while the rates of vulnerabilities #6 “Data recovery” and #9 “Insecure cryptography” are lowest rates in the study’s scenario. The other vulnerabilities have the average rates of increases that are not considered as sharp escalation.

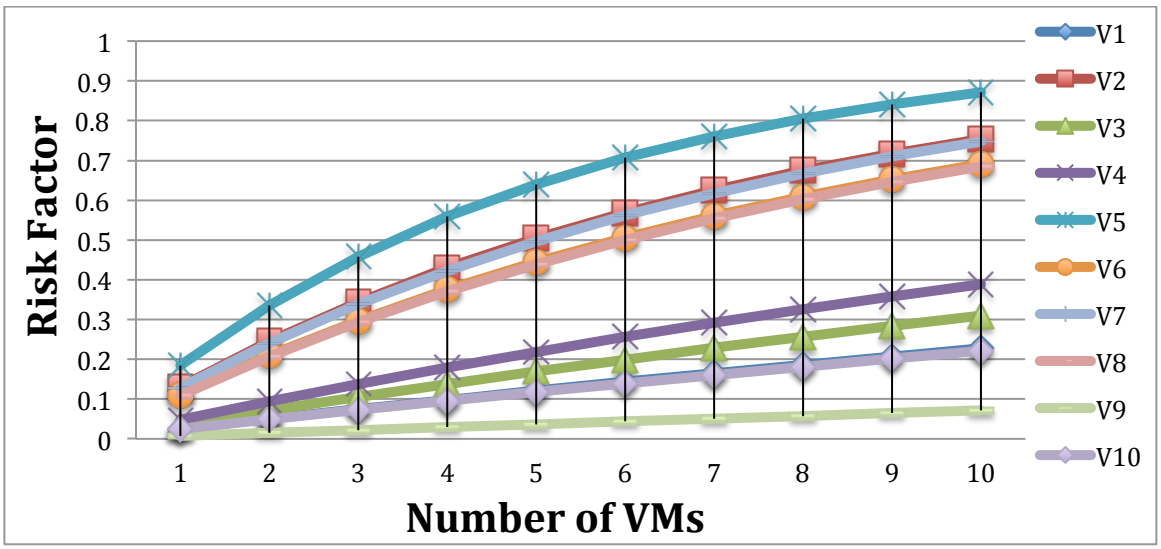

Figure 20: Risk factor Vs. Number of VMs

# Vulnerability	Risk Factor
1	0.150412217
2	0.568913115
3	0.207832352
4	0.265105099
5	0.695536388
6	0.509531338
7	0.561661049
8	0.503814898
9	0.046195712
10	0.14644147

Table 21: Risk factor per vulnerability

After this thesis states the general behavior of the risk factor, it calculates the average of the risk factor for every vulnerability. Table 21 shows the resulted outputs of the average of the risk factor for every vulnerability.

Figure 21 depicts the average of the risk factor based on the vulnerabilities. It is clear from the chart that vulnerability #5 “Data destruction policies” has the highest average risk factor at value of 0.69553. Vulnerabilities #1 “Data recovery”, #9 “Insecure cryptography” and #10 “Internet dependency” have the lowest averages that range from 0.046 to 0.150. The averages of other vulnerabilities fluctuate between 0.20 and 0.56.

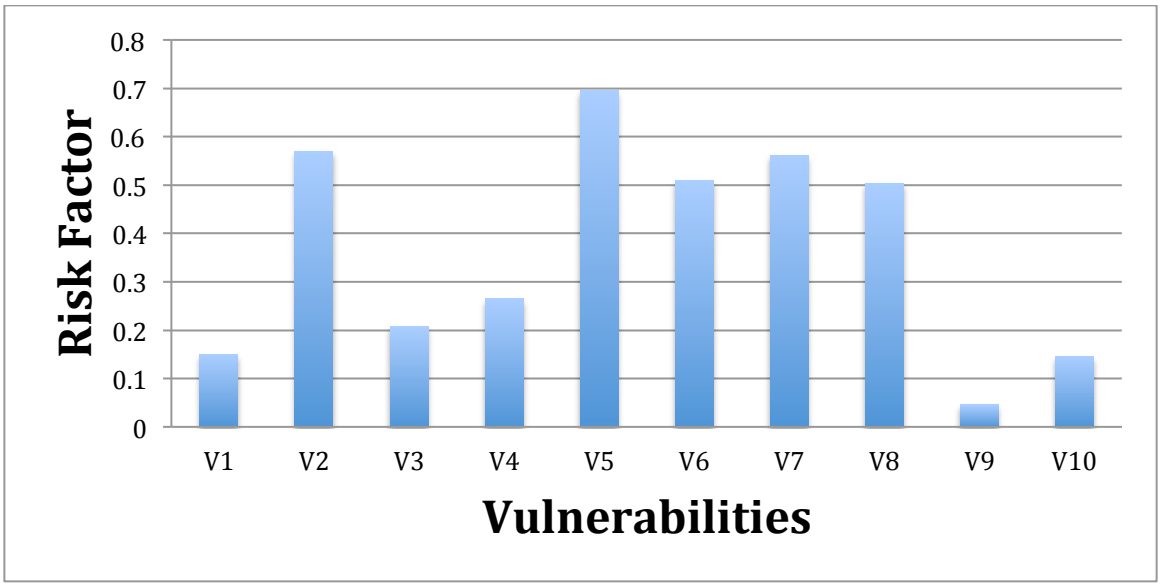

Figure 21: Risk factor per vulnerability

# VM	Risk Factor
1	0.577039428
2	0.821104355
3	0.924334195
4	0.967996348
5	0.986463717

6	0.994274686
7	0.997578418
8	0.998975766
9	0.99956679
10	0.999816769

Table 22: Risk factor per VM

On the other hand, Table 22 lists the total risk factor for each VM. The risk associated with each VM is the total risk factor that associated with each VM by all the 10 vulnerabilities. This study concludes these results by calculating the complete risks of all 10 vulnerabilities against one VM. Then each VM has an equal value of risk. Next, the total risk factor calculated while adding more VMs until 10 VMs consecutively. Thus, the calculation acquires risk values that range from 0.57 to 0.99. Then, the results are plotted to identify the behavior of risk factors while adding more VMs. Each VM has a risk factor of 0.577 and this point is the minimum risk value obtaining from the calculations.

After plotting the results on Figure 22, the chart demonstrates the clear behavior of the risk factor. It shows that risk factor is sharply increasing at the beginning. Then, the risk factor remains steady around a risk factor of 0.99. Figure 22 illustrates that while adding more VMs, the risk factor keeps increasing gradually until it is stabilized around 0.99, which is high level of risk. The main reason for this behavior is that some vulnerability has high value of risk factor. Thus, those specific vulnerabilities lead the total risk to be close to a value of 0.99 that indicates high level of risk.

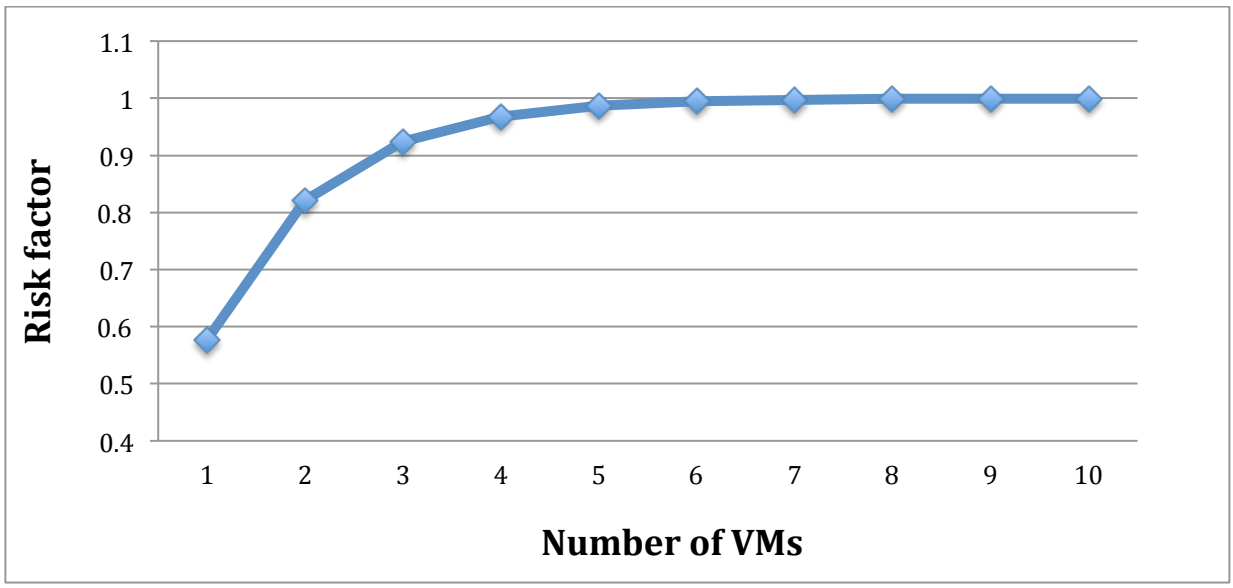

Figure 22: Risk factor per virtual machine

The used framework [8] has more tasks that are needed when you perform repetitive risk analysis in the same organization. Risk mitigation task is one of those steps, which tend to develop risk treatment plan to treat the current rated risks and find the treatment possibilities. This plan also includes risk rating after performing risk mitigation plan to see how much risk this scenario still has. Moreover, the plan contains the persons who are accountable to perform the risk mitigation recommendations. In this paper, general recommendations section is provided in page 60 instead of the risk mitigation plan. The last part of the framework [8] is to perform monitoring and review task, which can be done after performing the risk treatment plan. This task requires follow-up check by the cloud provider to ensure the risk treatment plan is completely implemented. Then, if the risk assessor finds new issues, he/she takes an action to treat the incidental issues. Check and Act is the last task of the Plan, Do, Check, and Act (PDCA) process model [8]. Those tasks are behind the objective of this research at this moment since one of the major objectives of this research is to find and assess the risk provided in cloud computing environments.

5. Experimental Results

In this study's scenario, the test cases are applied in a cloud environment that has up to 10 VMs. Nonetheless, most real cases would contain more than 10 VMs that perform different tasks. Thus, this study uses the existing results to estimate the behavior of the SLA-factors while adding more VMs. In cloud environment, scalability is one feature that is considered very beneficial to acquire more cloud resources, as you need and many cloud customers utilize this feature to provide more resources and ensure the service availability. As the customer utilizes more VMs, this study needs to ensure the behavior of the SLA factors and how the customers can be affected by having more cloud resources. Thus, the results are plotted in different charts and figures to illustrate the effects of those factors. Then, a curve fitting process is applied over the data to acquire the best fit of the data points. The produced line provides best fit to all the data points and it indicates the behavior of the SLA factors while adding more VMs. To achieve this task, this study uses the Matlab Curve Fitting tool [49] to produce the fitting line and all related figures. All the figures and discussion are provided in the following parts.

In term of the response time, this study performs different test cases to acquire the response times in different circumstances. First case is to see the behavior of the response time within the same subnet. Figure 23 depicts the distribution of the response time data within the same subnet per each VM. The response time has been calculated about 100 times for each VM. Figure 23 demonstrates that the response time fit-line remains stable as constant line between the 0.090 and 0.095 milliseconds. This fit-line indicates that while increasing the VMs in the same subnet, the response time remains constant for all the VMs in the cloud. This test is a case-specific for Amazon cloud services and it depends on infrastructure features of Amazon installation

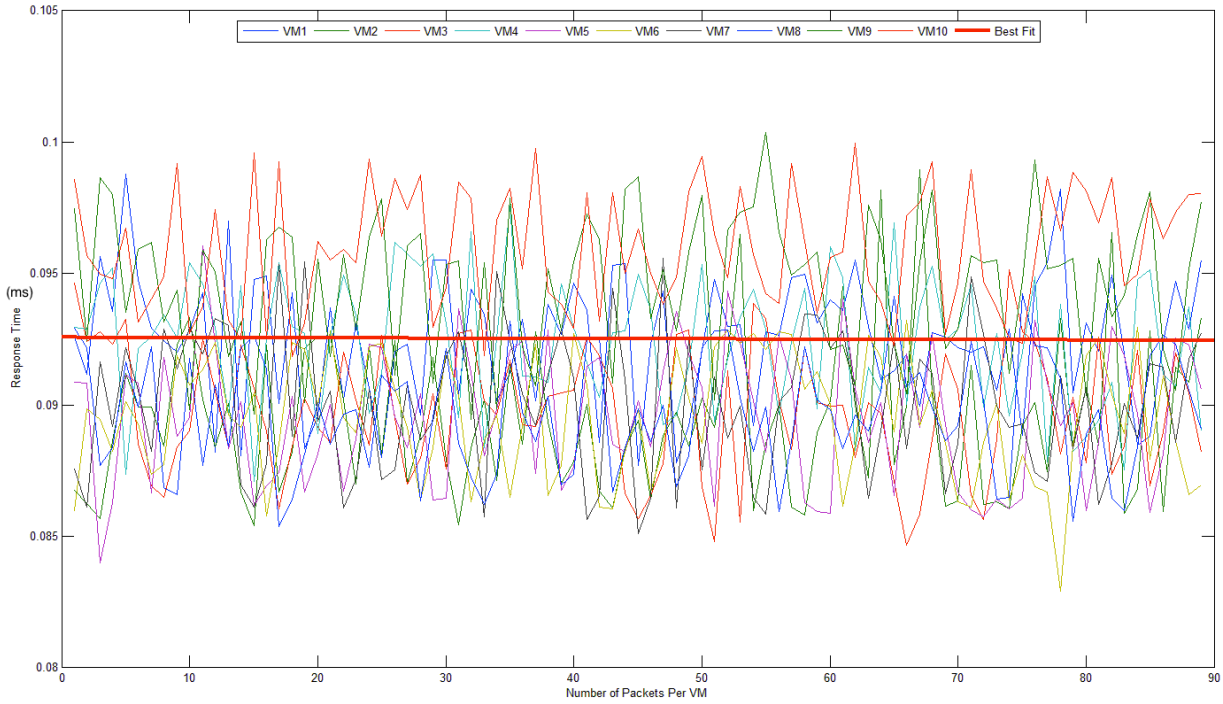

Figure 23: Fit-line of response time data within same subnet

Next, the research performs another test case, which is calculating the response time from other availability zone owned by the cloud provider. In this case, a VM in another availability zone (Europe zone) is set up. Then, the resulted data are plotted in a figure to produce the best-fit line. As previous case, Figure 24 illustrates the spreading of the response time data from another Amazon zone per each VM. The response time has been calculated about 100 times for each VM. Figure 24 proves that the response time fit-line remains unchanged about 0.17 second. This fit-line specifies that while adding more VMs in the cloud environment, the response time

continues persistent for all the VMs in the cloud. Similar to the previous case, this test is a case-specific for Amazon cloud services and it depends on infrastructure features of Amazon installation.

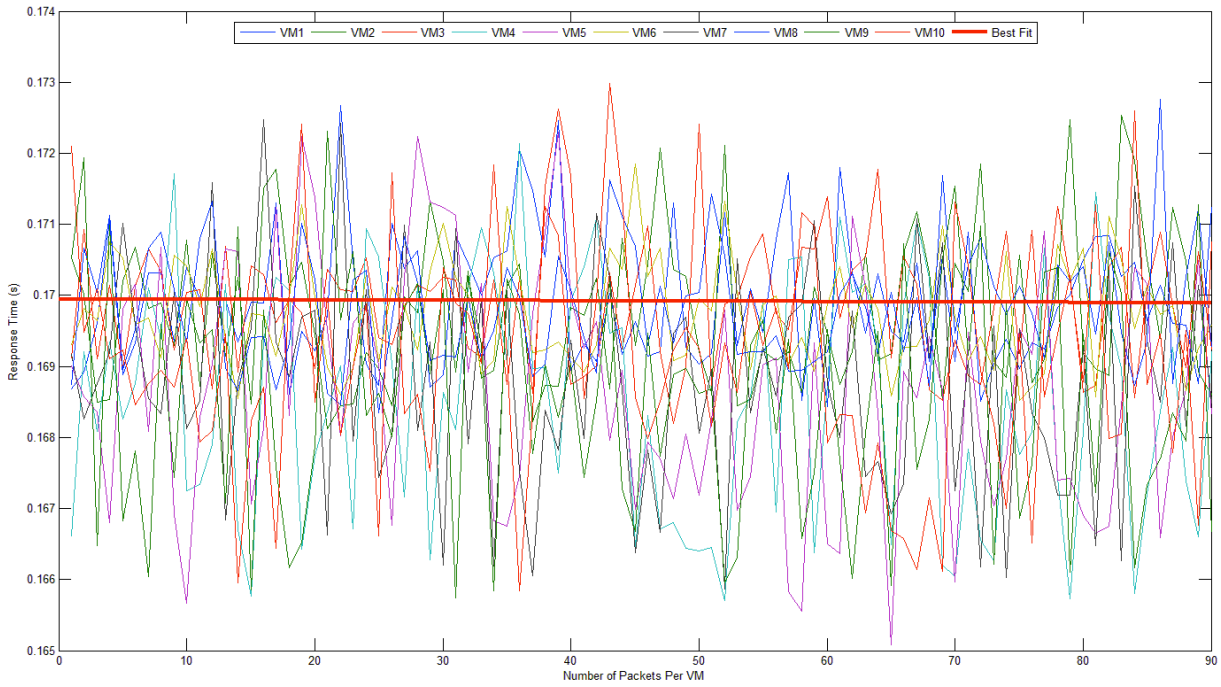

Figure 24: Fit-line of response time data from another availability zone

Then, this study implements a test case to find the response time between the physical network at RIT and the cloud environment that resides at Amazon zone (Oregon US). The results are placed in a figure to generate the fit-line that fits all data points. Like to the preceding test cases, Figure 25 clarifies the scattering of the response time data from RIT per each VM. Similarly, the response time has been calculated about 100 times for each VM. Figure 25 verifies that the response time fit-line is constant behavior between 0.090 and 0.095 second. This fit-line states that if the number of the VMs in the cloud environment increases, the response time remains constant for all the VMs in the cloud. Similar to the previous case, this test is a case-

specific for Amazon cloud services and it depends on infrastructure features of Amazon installation.

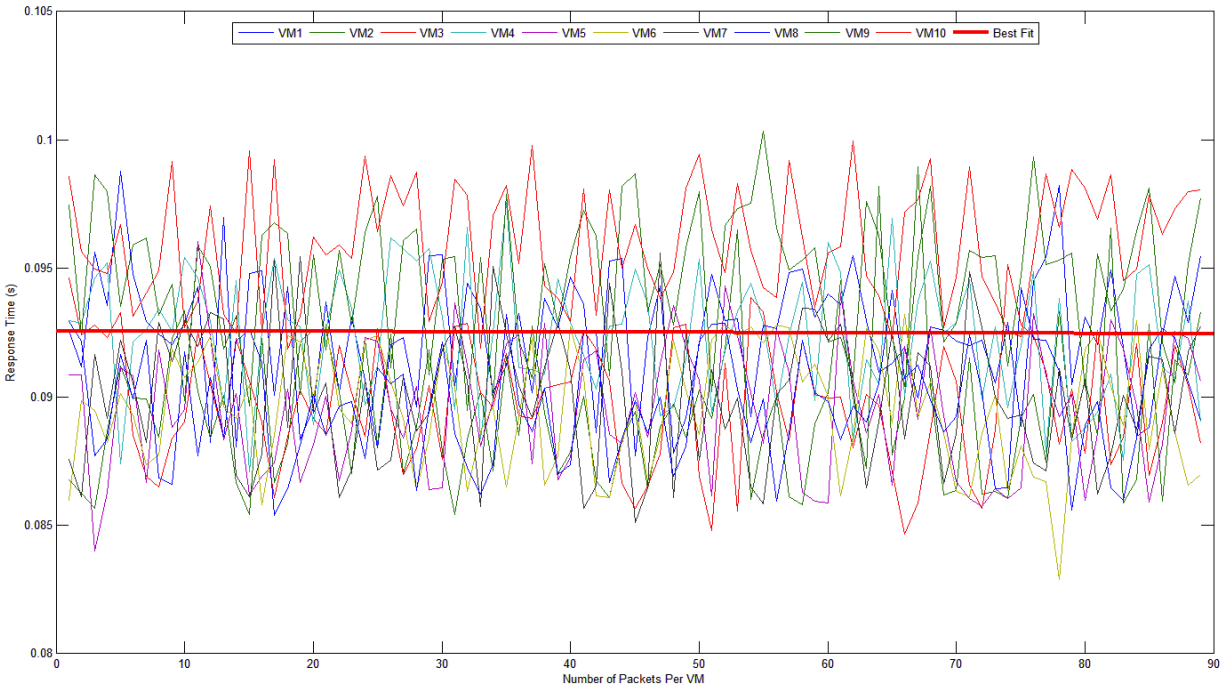

Figure 25: Fit-line of response time data from RIT

The response time in the three cases is constant but it differs in the time factor since the response time inside the subnet is extremely fast than other two cases. Also, the other two cases express the significance of the physical location of the cloud resources since connecting to the cloud within US is faster than connecting from another Amazon's zone outside the US.

Since the previous test cases use one-to-one response time, the next test case is related to calculate the end-to-end delay response time as done in section 4.1.4. In this case, there are two different scenarios. The first scenario is to assume the service request passes all the VMs and it's finally fulfilled by VM #10. The last VM does not provide the customer with any feedback. The resulted data are plotted to get the fit-line that fits all the data points. Thus, Figure 26 illustrates that the fit-line is steadily increasing while adding more VMs. After the first VM, the increase

factor is constant through all the VMs. Figure 26 shows that if more VMs are added, the response time of the service request increases by a constant factor.

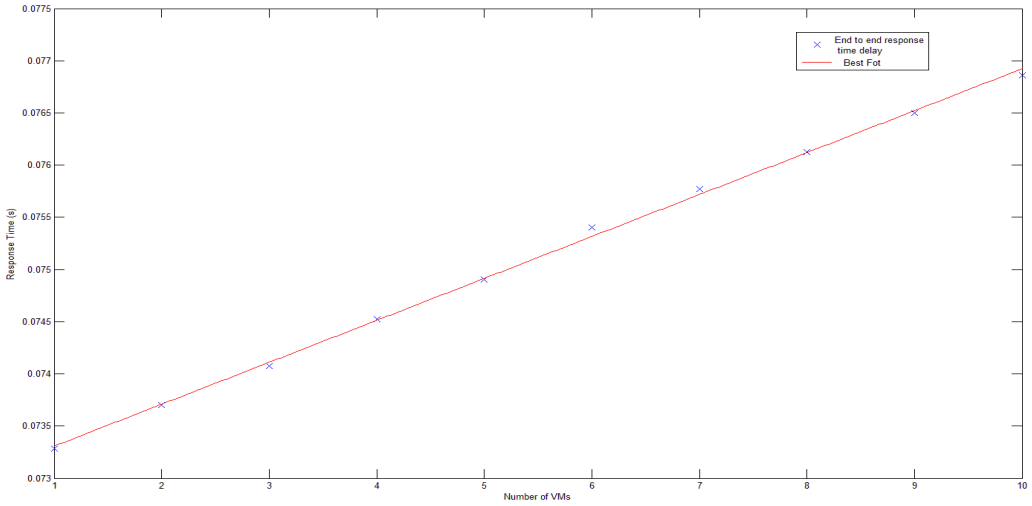

Figure 26: End-to-end response time without feedback

On the other hand, the second scenario assumes that the last VM responds with feedback to the customer. Figure 27 demonstrates the behavior of the best-fit curve of the scenario. While the distribution of data points shows constant behavior except for the last point, the best-fit curve is progressively increasing. The last point that appears as outlier that affects the fit curve behavior is the response time for the last VM's feedback. Thus, it is appears the response time is kept almost constant until a feedback task is required.

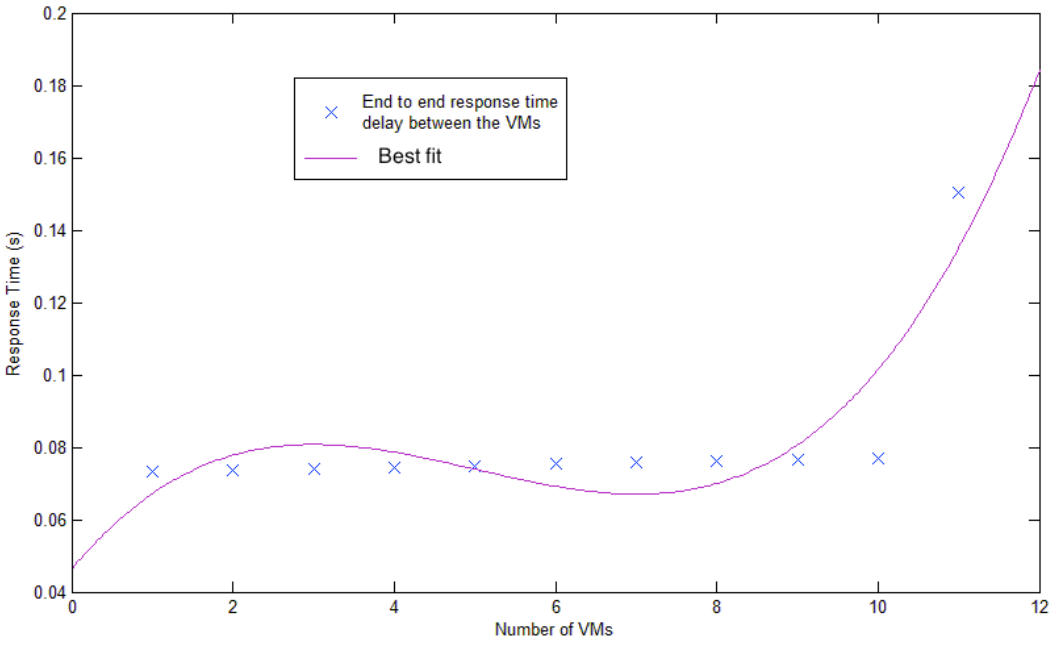

Figure 27: End-to-end response time with feedback

After discussing the first SLA factor in the previous part, this part discusses the second the SLA factor. Figure 9 shows that the total cost of cloud resources are gradually increasing while utilizing more cloud resources. Thus, the cloud customer needs to pay attention that using more cloud resources such as VMs, public IPs, cloud storage, or other computing services add more money to the bill. Also, the cloud customer should pay attention to charging policy since the pricing policy changes from cloud provider to another. For instance, Amazon AWS charges each VM per hour, which means if the customer uses the VM for 10 minutes only, the customer is charged for the whole hour.

Now, this part discusses the risk factor and its behavior while adding cloud resources. After all the results that get from section 4.3.2.2.3 are plotted, the best-fit curve that fits all the data points is generated. Figure 28 depicts that the fit curve is gradually increasing while adding more cloud resources that means adding VMs introduces more risk to the cloud environment.

Moreover, adding more VMs would defiantly increase the surface attack and introduce more risk. Thus, the risk factor increases while increasing the used cloud resources i.e. VMs.

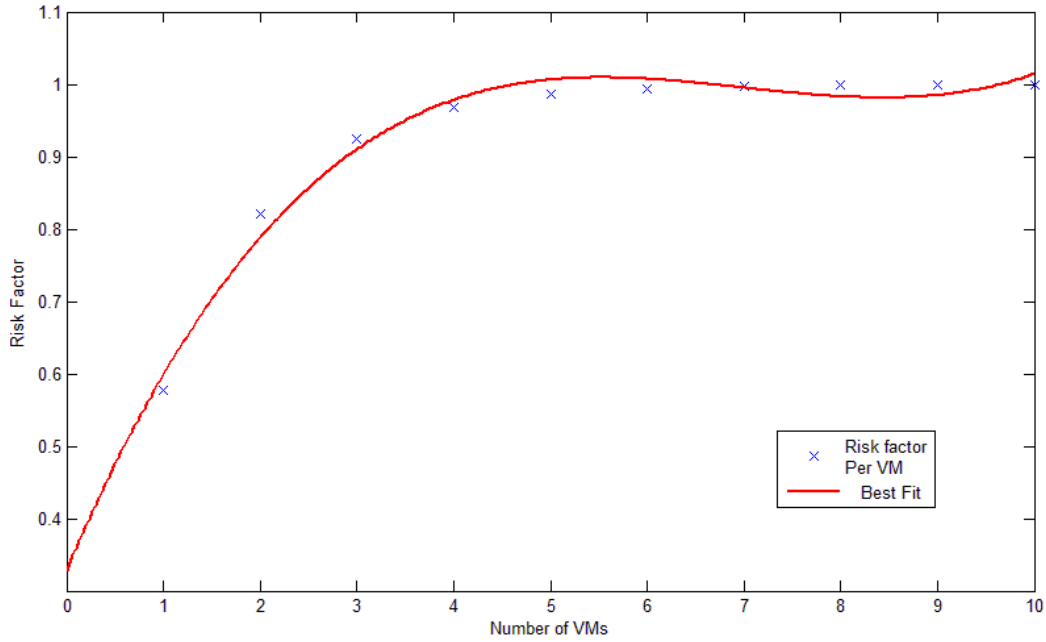

Figure 28: Best-fit curve for risk factor per VM

After this study examined the relationship between the SLA factor and cloud resources, it shows the relationship between the SLA factors. First of all, this research is going to study the relationship between risk factor versus the response time factor. Since the response time for individual VM is constant, in this case, this study uses end-to-end response time of a service request. Figure 29 illustrates that the risk factor and response time are directly proportional to each other. Thus, when the response time increases, the risk factor increases respectively. Increasing the response time would highly lead to risk of service unavailability.

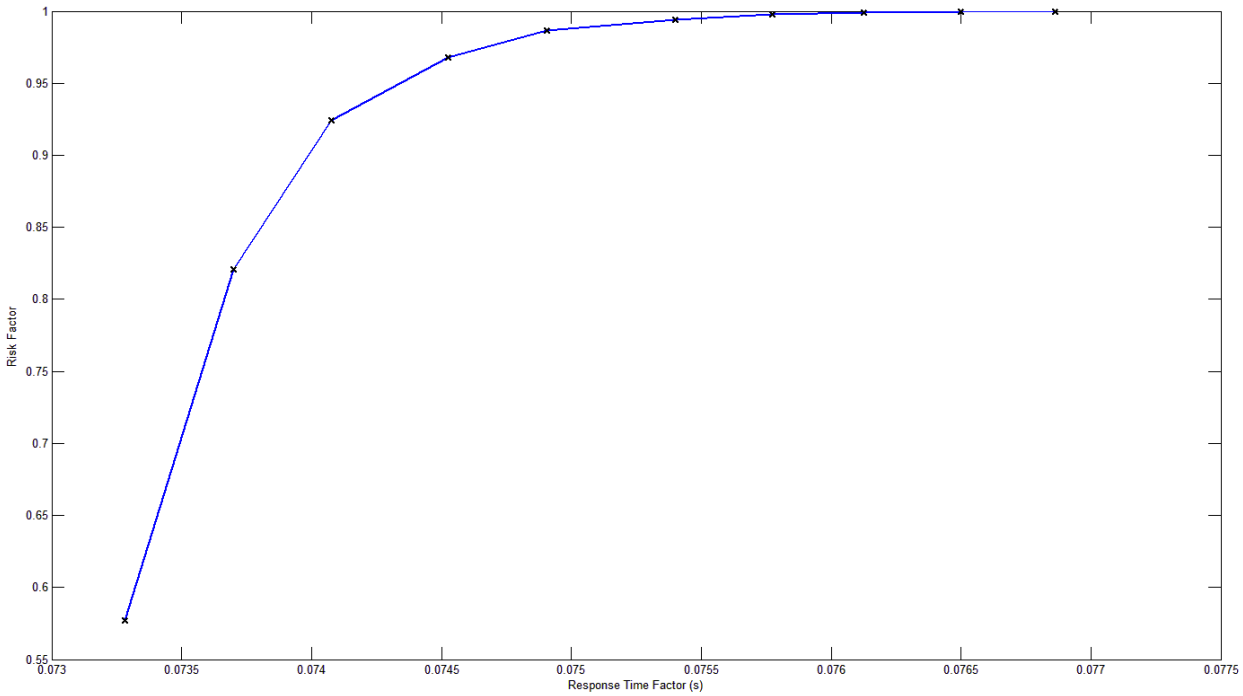

Figure 29: Risk factor vs. response time factor

To illustrate the relationship between those two factors, the fit-line between the two factors is generated to conclude the behavior of the line while adding more cloud resources. Figure 30 shows the fitting curve for the two factors is gradually increasing while adding more VMs.

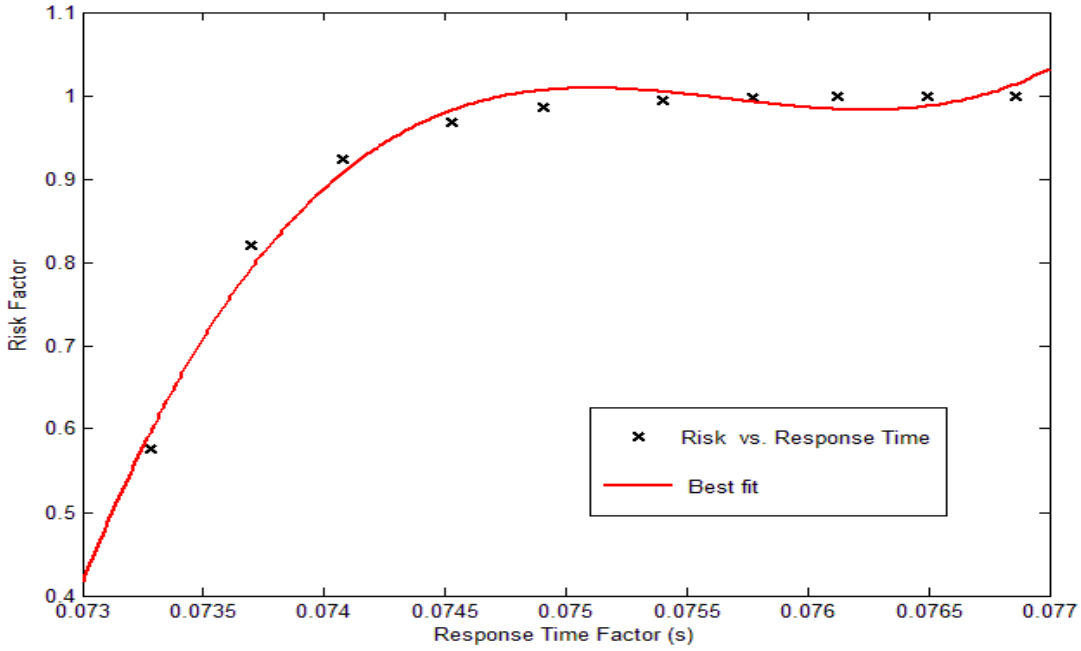

Figure 30: Best-fit curve for risk factor vs. response time factor

Then, this research shows the relationship between the risk factor and cost factor. Figure 31 expresses that if the risk factor and cost factors are directly proportional. This means that if the risk factor increases then, the cost factor is increasing correspondingly.

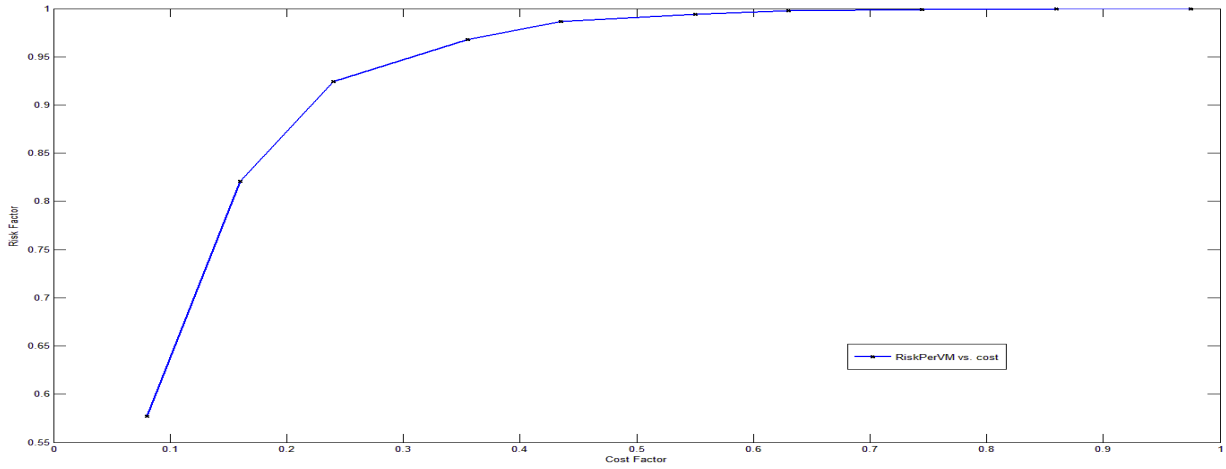

Figure 31: Risk factor vs. cost factor

Then, the best-fit curve that fits the resulted data points is generated. Figure 32 depicts the curve that estimates the future behavior of the relationship between the risk and cost factors. It is clear from the curve that as the risk increases, the cost factor increases too.

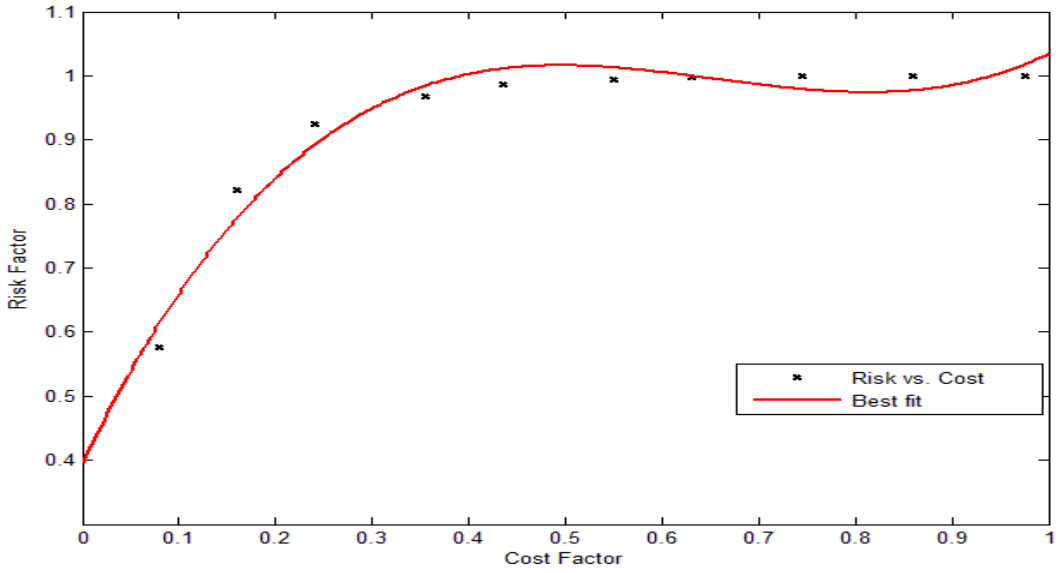

Figure 32: Best-fit curve for risk factor vs. cost factor

Finally, in this part, this research states in the relationship between the response time and the cost factors. Similarly, the response time of an end-to-end service request case is used to illustrate the relationship. Figure 33 indicates the relationship between the two factors since if the response time increases for all VMs, the cost factor keeps increasing respectively. Similar as the previous part, the increase here is also driven by the increase factor in the number of the VMs.

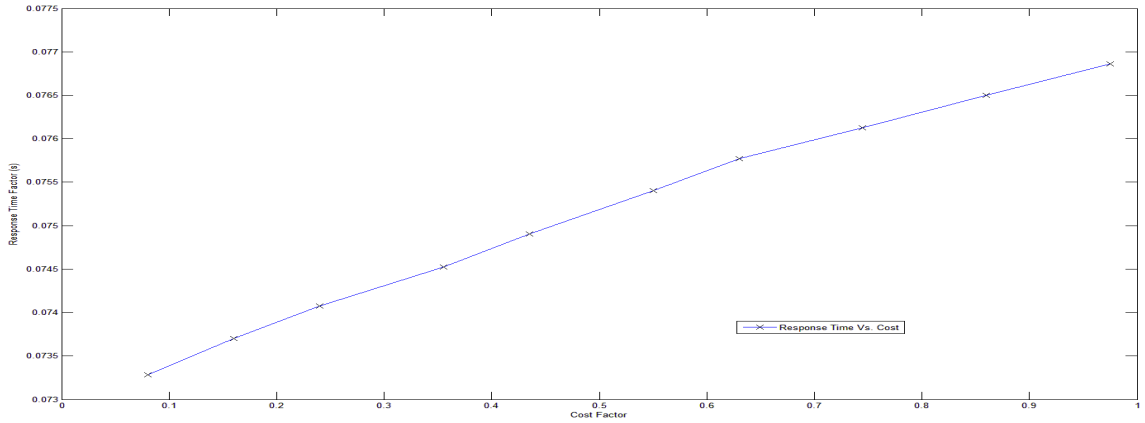

Figure 33: Response time factor vs. cost factor

Next, the fit-line that fits data points between the response and cost factors is acquired. Figure 34 indicates the fitting line that estimates the scalability of the relationship between the response time and cost factors. It is clear that the line is gradually growing as the two factors keep increasing. Thus, the relationship between those two factors is directly proportional.

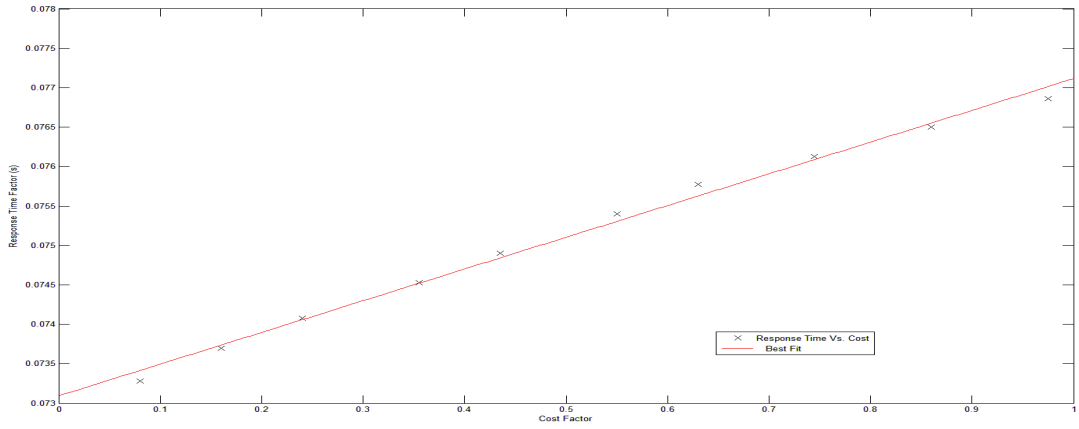

Figure 34: Fit-line for response time factor vs. cost factor

6. Recommendations

This research shows the importance of the relationship between the SLA factors. After this study analyzes those factors, it comes up with important issues and findings. First of all, before any customer decides to move to a cloud environment, the customer should perform comprehensive analysis for the SLA factors. As seen in this research, those factors can behave according to different reasons. Understanding those factors and their significance would provide the customer with better knowledge to take decent decisions in a cloud-computing environment. Moreover, this research indicates that the current public cloud environments are areas of risk where a customer needs to think before taking any decisions. The cost factor should be investigated and analyzed to state its affect in an organization budget. The customer should read the pricing policy very carefully to understand all the cost provisions. Moreover, the customer should ensure how the cost factor in the SLA is met and how to measure this factor very carefully.

This research states the essential role of the response time. The response time is an important factor to ensure the availability of the services. This research shows the effect of the physical location of the cloud environment and how that can affect the service request performance. Also, the research states that the best cloud provider should provide good response time with at least constant value. Ensuring the response time is part of ensuring the quality of the service (QoS) that is used to evaluate the SLA factors.

Besides the response time and cost factors, this research concentrates more in risk factor because most of the SLA in cloud services lacks this factor. Thus, this study shows the importance of this factor and how it is related to other SLA factors such as response time and cost factors. This research concludes that the risk factor should be brought to the table of

negotiation between the cloud providers and their customers. The customers should engage a risk management team in negotiation to provide broad vision about the ambiguous areas in SLAs such as the risk factor. Also, the cloud providers should hire risk management team from a third party provider to analyze its environment regularly to build trust relation between the service and its customers. This includes ensuring if the cloud providers meet the compliance requirements for different laws and standards. The final results of the risk analysis should play a significant role in making the decision, negotiating, and finalizing the SLAs. Then, the cloud provider and customer should both ensure the implementation and monitoring of the SLA to avoid any disruptions or violations.

7. Future Work

Risk management in cloud environment has been considered an active area in cloud computing research recently. There are different points in the future work that may be done to improve or contribute to this work. First, the future work in this topic may include different SLA metrics and study their relationship to the risk metric. Those metrics may include trust, violation ratio, availability, and elasticity. Then, the future work may aim to find the relationships between the risk factor and those metrics. Moreover, future work may perform different studies to find the practical effects of the risk management process in SLA negotiation and enforcement processes. Since this research implements a private cloud using a public cloud provider, future work may implement different scenarios such as using public cloud environment or implement on-promise cloud environment. Then, the same steps may be performed to the new scenarios and compare them to mentioned scenario in this paper. Also, the future work may implement cloud service models such as Software as a Service (SaaS) or Platform as a Service (PaaS). Then, the same

steps used in this paper may be employed against those service models. Furthermore, the future work may include in-depth risk analysis for SLA real cases that are published by service provider such as Amazon.

8. Conclusion

In conclusions, this paper discussed some issues in cloud computing that have not been discussed frequently. This research implemented SLA-based risk analysis in cloud computing environments. The research evaluates important SLA parameters such as response time, cost, and risk factors. As a result, this paper indicated the relationship between the risk parameter and other SLA parameters such as response time and the cost. This paper declares the importance of the risk management requirement as an SLA parameter. Different consequences resulted from this analysis state the important relation between the risk factor and other SLA metrics such as the response time and cost factors. This paper indicates the effect of lacking risk parameter in the current SLA provided by most cloud providers. Also, it provides customer with risk analysis for various SLA factors and this helps the customer to make a better decision before moving to the cloud environment. Finally, the paper states that there are important relationships between all the three SLA factors and all those relationship indicate the importance of the risk factor in any SLA.

9. Bibliography

[1] M. Alhamad, T. Dillon, and E. Chang, "SLA-Based Trust Model for Cloud Computing," in *Network-Based Information Systems (NBiS), 2010 13th International Conference*, 14-16 Sept., pp. 321-324.

[2] M. Alhamad, T. Dillon, and E. Chang, "Conceptual SLA framework for cloud computing," in *Digital Ecosystems and Technologies (DEST), 2010 4th IEEE International Conference*, 13-16 April 2010, pp. 606-610.

[3] Adil M. Hammadi and Omar Hussain, "A Framework for SLA Assurance in Cloud Computing," in *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference*, 26-29 March 2012, pp. 393-398.

[4] Yun Chi, Hyun Jin Moon, Hakan Hacigumus, and Junichi Tatemura, "SLA-tree: a framework for efficiently supporting SLA-based decisions in cloud computing," in *In Proceedings of the 14th International Conference on Extending Database Technology (EDBT/ICDT '11)*, New York, NY, USA, 2011, pp. 129-140.

[5] Jahyun Goo, "Structure of service level agreements (SLA) in IT outsourcing: The construct and its measurement," in *Information Systems Frontiers 12*, April 2010, pp. 185-205.

[6] M. Hedwig, S. Malkowski, and D. Neumann, "Risk-Aware Service Level Agreement Design for Enterprise Information Systems," in *System Science (HICSS), 2012 45th Hawaii International Conference* , Jan. 2012 , pp. 4552-4561.

[7] P. Bhoj, S. Singhal, and S. Chutani, "SLA management in federated environments," in *Comput. Netw. 35*, January 2001, pp. 5-24.

[8] Xuan Zhang, N. Wuwong, Hao Li, and Xuejie Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference*, June 29 2010-July 1 2010, pp. 328-1334.

[9] Yeni Yuqin and Li Helgesson, "Integrating SLAs into IT Risk management in public service organizations," in *Services Computing Conference, 2009. APSCC 2009*, 7-11 Dec. 2009, pp. 119-125.

[10] J. Morin, J. Aubert, and B. Gateau, "Towards Cloud Computing SLA Risk Management: Issues and Challenges," in *System Science (HICSS), 2012 45th Hawaii International Conference*, 4-7 Jan. 2012, pp. 5509-5514.

[11] The European Network and information Security Agency. (2009, Nov) Cloud Computing Risk Assessment. [Online]. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[12] Cloud Security Alliance. (2011, October) Security Guidance for Critical Areas of Focus in Cloud Computing v3.0. [Online]. https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[13] Chee Shin Yeo and R. Buyya, "Integrated Risk Analysis for a Commercial Computing Service," in *Parallel and Distributed Processing Symposium, 2007. IPDPS 2007*, 26-30 March 2007, pp. 1-10.

[14] H. Waldman and D.A.A. Mello, "On the risk of non-compliance with some plausible SLA requirements," in *Transparent Optical Networks, 2009. ICTON '09. 11th International*

Conference, June 28 2009-July 2 2009, pp. 1-4.

[15] Dominic Battré , Georg Birkenheuer, Matthias Hovest, Odej Kao, and Kerstin Voss , "Applying Risk Management to Support SLA Provisioning," in *Proceedings of the Cracow Grid Workshop (CGW)*, 2008.

[16] FERMA. Risk Management Standard. [Online]. http://www.ferma.eu/risk-management/standards/risk-management-standard/

[17] R. Clemente, M. Bartoli, M.C. Bossi, G. D'Orazio, and G. Cosmo, "Risk management in availability SLA," in *Design of Reliable Communication Networks, 2005. (DRCN 2005). Proceedings.5th International Workshop*, 16-19 Oct. 2005, p. 8.

[18] Bo Yang, N.A. Aran, Sai Zeng, and R. Puri, "SLA-driven applicability analysis for patch management," in *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium*, 23-27 May 2011, pp. 438-445.

[19] P Patel, A. Ranabahu, and A. Sheth, "Service Level Agreement in Cloud Computing," in *Cloud Workshop at OOPSLA*, 2008.

[20] M. Hovestadt, Odej Kao, and Kerstin Vouu, "The First Step of Introducing Risk Management for Prepossessing SLAs," in *Services Computing, 2006. SCC '06. IEEE International Conference*, 18-22 Sept. 2006, pp. 36-43.

[21] Rajkumar Buyya and Manzur Murshed, "GridSim: A Toolkit for the Modeling and Simulation of Distributed Resource Management and Scheduling for Grid Computing," in *The Journal of Concurrency and Computation: Practice and Experience (CCPE)*, vol. 14, Nov.-Dec., 2002.

[22] Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglaz, Cesar A. F. De Rose, and Rajkumar Buyya, "CloudSim: A Toolkit for Modeling and Simulation of Cloud Computing Environments and Evaluation of Resource Provisioning Algorithms, Software," in *Practice and Experience (SPE)*, vol. 41, New York, USA, January, 2011, pp. 23-50.

[23] Amazon Web Services LLC. Amazon Virtual Private Cloud (Amazon VPC). [Online]. http://aws.amazon.com/vpc/

[24] Amazon Web Services LLC. AWS Support FAQs. [Online]. http://aws.amazon.com/premiumsupport/faqs/#sfhctime

[25] Amazon Web Services LLC. Amazon Elastic Compute Cloud (Amazon EC2) - Pricing. [Online]. http://aws.amazon.com/ec2/#pricing

[26] National Institute of Standards and Technology (NIST). (2002, July) isk Management Guide for Information Technology Systems. [Online]. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[27] Edward Humphreys, *Implementing the ISO/IEC 27001 Information Security Management System Standard*., 2007.

[28] Amazon Web Services LLC. (2012, July) Amazon Web Services: Risk and Compliance. [Online]. http://d36cz9buwru1tt.cloudfront.net/AWS_Risk_and_Compliance_Whitepaper.pdf

[29] Carnegie Mellon University Software Engineering. (2008, July) OCTAVE Method. [Online]. http://www.cert.org/octave/octavemethod.html

[30] Cloud Security Alliance. (2010, March) Top threats to Cloud Computing V1.0. [Online]. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[31] Michael Whitman. (2003, August) Threats to Information Security. [Online]. http://classes.soe.ucsc.edu/cmps122/Spring04/Papers/whitman-cacm03.pdf

[32] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," in *Security & Privacy*, vol. 9, 2011, pp. 50-57.

[33] Mervat Adib Bamiah and Sarfraz Nawaz Brohi, "Seven Deadly Threats and Vulnerabilities in Cloud Computing ," *INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES*, 2011. [Online]. http://www.ijaest.iserp.org/archieves/15-Jul-15-31-11/Vol-No.9-Issue-No.1/16.IJAEST-Vol-No-9-Issue-No-1-Seven-Deadly-Threats-and-Vulnerabilities-in-Cloud-Computing-087-090.pdf

[34] Michael E. Whitman and Herbert J. Mattord, *Management of Information Security*. Boston, MA, United States: Cengage Learning, 2010.

[35] Amazon Web Services LLC. (2009, November) Linux kernel vulnerability in certain EC2 AMIs. [Online]. http://aws.amazon.com/security/linux-kernal-vulnerability-in-certain-ec2-amis/

[36] Amazon Web Services LLC. (2008, May) Thread: SSH host key paranoia. [Online]. https://forums.aws.amazon.com/thread.jspa?threadID=21867

[37] Amazon Web Services LLC. (2008, June) Amazon Elastic Compute Cloud. [Online]. http://docs.amazonwebservices.com/AWSEC2/2008-02-01/GettingStartedGuide/index.html?WhatsNew.html

[38] Amazon Web Services LLC. (2011, May) Overview of Security Processes. [Online]. http://d36cz9buwru1tt.cloudfront.net/pdf/AWS_Security_Whitepaper.pdf

[39] Henry Blodget. (2012, July) Amazon's Cloud Crash Disaster Permanently Destroyed Many Customers' Data. [Online]. http://articles.businessinsider.com/2011-04-28/tech/29958976_1_amazon-customer-customers-data-data-loss

[40] Amazon Web Services LLC. (2012, June) Microsoft Windows RDP Vulnerability. [Online]. http://aws.amazon.com/security/security-bulletins/microsoft-windows-rdp-vulnerability-06152012/

[41] Amazon Web Services LLC. (2012, June) Xen security advisories. [Online]. http://aws.amazon.com/security/security-bulletins/xen-security-advisories/

[42] Amazon Web Services LLC. (2012, September) Xen security advisories. [Online]. http://aws.amazon.com/security/security-bulletins/xen-security-advisories-09112012/

[43] Amazon Web Services LLC. Amazon Simple Storage Service FAQs. [Online]. http://aws.amazon.com/s3/faqs

[44] Om Malik. (2012, June) Severe storms cause Amazon Web Services outage. [Online]. http://gigaom.com/cloud/some-of-amazon-web-services-are-down-again/

[45] Om Malik. Parts of Amazon Web Services suffer an outage. [Online]. http://gigaom.com/cloud/did-amazons-web-services-go-down/

[46] Derrick Harris. (2011, April) Here's What Amazon's Outage Looked Like. [Online]. http://gigaom.com/cloud/heres-what-amazon-outage-looked-like/

[47] Mike Gunderloy. (2008, July) S3 Outage: the Aftermath. [Online]. http://gigaom.com/collaboration/s3-outage-aftermath/

[48] Amazon Web Services LLC. Amazon EC2 Service Level Agreement. [Online].

http://aws.amazon.com/ec2-sla/
[49] MathWorks. Curve Fitting Toolbox. [Online].
http://www.mathworks.com/products/curvefitting/

Appendix

List of Tables

List of Figures

Scripts

Response_Time_Server.pl

```
/*
By Mohammed Almathami, RIT
This script tends to calculate the response time between two computers.
*/

#! /usr/bin/perl
use warnings;
use Net::Ping;
use Time:HiRes;

# Variables
#IP address of the target machine
```

```
#A loop can be used to test multiple IPs at the same time
@hosts = ("50.112.153.2");


#The sum of the response time of all requests
$sum=0;

#The average of the response time
$avg=0;

#Start loop of IPs
foreach $host (@hosts) {

#for loop to send multiple TCP Ping to each machine
for ($count = 1; $count <= 100; $count++)
{

#Establish the packet
$p = Net::Ping->new("syn");

#Identify the listening port on the server
$p->port_number(99999);

$p->hires();

#Send TCP Ping
$p->ping($host);

#Get the info from the ACK of the packet
($host,$rtt,$ip) = $p->ack($host);

#Convert millisecond to seconds $MS = $rtt / 1000 if needed
$MS = $rtt;

#Print the results
print " at $count Machine's IP @ [$ip] responds in $MS seconds.\n";

#The sum of the response time
$sum = $sum + $MS;

$p->close();
}
#For loop ends here

#Find the average of the response time by dividing the sum of the response time by the number of the
packets
$avg = $sum / 100;

# Print the results
```

```
print " The sum of the response time is: $sum seconds.\n The average of the response time is: $avg seconds.\n";

#End of IPs
}
```

Listener.pl

```
/*
By Mohammed Almathami, RIT
This script tends to listen on port 99999 on the machine that is being tested for the response time.
*/

#!/usr/bin/perl -w
use strict;
use warnings;
use IO::Socket;

# Variables
# Identify the listening port on the server
my $PORT = 99999;

#Start the listener on the machine
my $listener = IO::Socket::INET->new(
        Proto     => 'tcp',
        LocalPort => $PORT,
        Listen    => 5,
        Reuse     => 1)
or die "can't setup listener";

print "This machine is now listening for a TCP connection on port 99999\n";

while (my $connection = $listener->accept()) {close $connection;}
```