ABSTRACT

Formal Model to Reduce the Risk of Cloud Outages

By Komal Hotwani

December, 2014

Director of Thesis: Dr. Nasseh Tabrizi

Major Department: Computer Science

Cloud outages have become very common in recent years as many companies adopt hosted services. One of the major reasons for cloud outages is the service level for availability, reliability, security not being met as mentioned in a service level agreement. The main purpose of this thesis is to introduce a model to calculate, control and reduce the risk of cloud outages. The objective is also to help consumers make an educated decision and to help them select a right providers. In order to understand the granularity of risk of cloud outage and its impact in the current cloud business, a survey was conducted to support our claim that there is a strong

need to calculate the risk associated with a service before signing a service level agreement. Survey responses also helped to prioritize the service level parameters used in our model from the consumer point of view.

Our model considers requirements, priorities, service level parameters, and cost as inputs. This model implements a modified version of a well-known mathematical model, Weighted Product Model (WPM) to compare different providers and to sort the eligible cloud providers. The methodology also uses Value At Risk (VAR) term, which is widely used term in the financial industry. The final output of the model, gives the risk value associated for a service for each parameter. Additionally, the model shows the probabilistic value for occurrence of cloud outage. The resulted information will be helpful for consumers to select a right cloud service provider with a minimum risk of cloud outage. This information will bring visibility of risk between a provider and a consumer helping to reduce the risk of cloud outage after the adoption of cloud service.

Formal model to reduce the risk of Cloud Outages

A Thesis

Presented to the Faculty of the Department of Computer Science

East Carolina University

In partial fulfillment of the Requirements for the degree

Master of Science in Software Engineering

By Komal Hotwani, December, 2014

Formal Model to Reduce the Risk of Cloud Outages

By

Komal Hotwani

APPROVED BY:

DIRECTOR OF
THESIS: ____

Nasseh Tabrizi, PhD

COMMITTEE MEMBER: ____

Karl Wuensch, PhD

COMMITTEE MEMBER: ____

Mark Hills, PhD

CHAIR OF THE DEPARTMENT
OF COMPUTER SCIENCE: ____

Karl Abrahamson, PhD

DEAN OF THE
GRADUATE SCHOOL: ____

Paul J. Gemperline, PhD

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF EQUATIONS

CHAPTER 1: INTRODUCTION

Cloud computing recently received much attention in industries and research communities. Companies can pay a cloud vendor for a service in a pay-as-you-go manner. These services can be software, platform, or even infrastructure service. Although the future of cloud looks promising, there are several reasons including risk of cloud outages [24] as why companies are reluctant to change their business to the cloud. Technology related news and articles [24] describe that cloud can be too precarious for implementing service level agreements. At the same time, there are business organizations, which overlook or are uninformed to consider the risk involved with cloud outages during the migration process. There can be different reasons for cloud outages such as hardware failure, loss of power, network connectivity issues, data center going offline, failed backups, software bugs, denial of service (DoS) attack, or human error [22]. There are known as well as unknown causes for cloud outages. The word cloud brings in mind a heavenly fantasy and as a concept that there is lot to know about the actual reality. The cloud is sold as this magical thing that works and is totally reliable. It is similar to a thought where we drop those bulky servers and get a big white hard drive in the sky [21]. Someone else handles the upkeep and allows us to put the data where they want. When we gain in avoiding upkeep, we definitely lose in control of this service. The truth is that buying through the cloud is another way of buying computing and computing is inherently flawed. The author JR Raphael suggests [21] if we want to make sure that these flaws do not hurt us, we have to plan ahead. The scope of this thesis is to understand cloud outages, reasons for cloud outages, and propose a solution to reduce the risk of cloud outages.

1.1 Cloud Outage

The simplest definition for cloud outage is a period of time during which cloud services are unavailable [22] for this research we consider, cloud outage as an unavailable service due to any reason. Even the best cloud companies have faced cloud outages [14]. The cloud can be seen as a service, which is provided by the cloud provider and consumed by the end user. As more companies are migrating and depending on cloud services, the impact of a single cloud outage is increasing. Most solutions offer a way to better plan for cloud outages, but often they are not applicable to all businesses. Cloud outage can also be referred as a low quality cloud service resulting in low degrees for availability of service, running slowly, poor performance of a service, insufficient data storage and providing an insecure environment to store data. If this continues, cloud service consumers may stop using cloud services and look for alternative solutions. On the other side, if the cloud service consumption is utilized well and performed well, more users can use it at the same time. Cloud outages occur every year as supported by the studies including [24] shows that there are many unreported cloud outages. To remedy the cloud outages some companies' implemented High Availability (HA) features and Disaster Recovery (DR) processes, but still there are other unique challenges with cloud computing. Cost analysis is a lot more complicated for cloud services compared to regular data centers.

The challenge here is to compute the cost based on the consumptions of static computing. An instantiated virtual machine has become the unit of cost analysis rather than the underlying physical server [2]. Furthermore, cloud consumers do not have control over the underlying computing resources [2]. They do need to ensure the quality, availability, reliability and performance of these resources when they move their core business functions onto the cloud. There are several challenges involved with service level agreements. We will consider these challenges in our research. Service can be of any type, but infrastructure downtime is inevitable in cases such as equipment failure, unexpected software bugs, and natural disasters. There were several reported cloud outages in the year 2013 [18]. It was not just a single outage; there were series of hard outages for the online insurance marketplace [18]. Downtime is particularly costly in the financial sector, as many Canadians learned in January 28, 2013 when they were unable to use their visa cards for much of the day due to a data center power outage at Total System Services Inc. (TSS), one of the largest processors of card payment transactions in North America. Yahoo Mail experienced up to four days of availability problems in December 2013 prompting a personal apology from Yahoo CEO Marissa Mayer [18]. Unfortunately, the outage was much more complex than it seemed at first, which is why it took several days to resolve the issue. CEO blamed a particularly rare hardware outage as a reason for downtime [18]. Windows Azure, Xbox, Blue Host faced the outage during the same year [18]. Amazon cloud service showed a message “Http/1.1 Service Unavailable” on January 31, 2013 with duration of 49 minutes [21]. Since, Amazon is an online retailer it depends on online orders to do business. Looking at the little fancy math some industry watchers estimated that Amazon could have potentially suffered close to $5 million in missed revenue [21]. Dropbox faced the outage for about an hour on January 10, 2013 [18], informing customers via twitter that all client syncing and file uploading would be unavailable for approximately the next hour. Facebook was down for about two to three hours on January 28, 2013 [18], which didn’t go unnoticed. Microsoft Bing was down for about two hours on February 1, 2, 2013 [18]. According to Microsoft, scheduled network configuration change was the root cause of the issue [21]. Cloud fare is a company which revolves around protecting and accelerating sites around the web, but on morning of March 3, 2013 the company’s own site and all of its services kicked the bucket, taking down some 785,000 other sites including WikiLeaks, 4chan, and some government sites along with them [21].

The impact of cloud outages is not only on internal users, but also on a company's reputation, stakeholders, and partners [21]. It impacts revenue, credibility, productivity and trust. When consumers become increasingly dependent upon the cloud for application, they demand reliable and easy access to their data but whether it is a public cloud, or own data center still downtime, unavailability of a service or a cloud outage is inevitable.

1.2 Scope and Focus

Cloud services allow consumers or organizations to give away control to the Cloud Service Provider (CSP). Anytime the cloud consumer relinquishes control, consumer adds a measure of risk to the current business situation. From the risk management perspective, the main challenges are with data security, availability, and reliability while moving to cloud. Cloud outages directly relate to the quality of cloud services. Hence, it is important to consider these service level parameters for critical decision-making and to understand the cost effectiveness of cloud services. As described in this whitepaper [10] the key features while assessing the benefits of cloud services include availability, security, and reliability measures with data loss. For measuring availability the consumer should know in-depth details about who is the network provider like past history, measured performance, measured downtime, and measured committed availability hours in the past by the network provider. Similarly, for security the details required from the past history of the provider could be details like which security certification will be applied to the service. In order to make a best decision, consumer should know how the service will recover data loss for consumers. This means reliability is another important factor to consider with cloud services. Service with high availability and high reliability will definitely increase the benefits of cloud services for a consumer.

The underlying agenda for this research is to know the important characteristics of a service, which directly contribute to minimizing risk of cloud outages. Idea here is how to measure the risk factor involved with each key performance indicators or important characteristics of a service. The goal is to understand the important steps that a cloud consumer should take in order to minimize or avoid the risk involved due to cloud outages. Much government, industries are trying to come up with standards, but since the cloud computing is a relatively recent phenomenon, the cloud process standards has begun only recently. Although cloud standards are being developed globally, the US NIST [20] is also in the process of launching an online portal to identify gaps in cloud standards to accelerate the development of standards for security, interoperability and portability

When organizations face cloud outages, the most common given reason to the consumers is service quality parameters did not meet the service levels as mentioned in a service level agreement (SLA). This thesis will focus on this area of a cloud service. The SLA is an important contract which brings visibility between a consumer and a provider while deciding the values for service levels for each parameter. This thesis is further supported on an idea to bring more visibility about unknown risk of cloud outage between cloud provider and cloud consumer. It will also consider important challenges from the consumers and will consider current business scenarios to analyze the risk of cloud services. However,

This thesis will not involve any real time cloud deployed services by any cloud providing organizations. The major focus is to present a solution, which educate the consumer as well as the provider very clearly about the risk of cloud outage involved for a cloud service. The ultimate goal is to develop a formal model, which can help consumers to take simpler, well-versed and accurate decision to select the right service provider, which involves minimum risk of cloud outage.

1.3 Structure of Thesis

Chapter 1 introduces the problem statement, described cloud outages and provided a brief description about the focus and scope of this thesis.

Chapter 2 provides the background and detailed study for cloud outages and its impact in cloud industry today

Chapter 3 describes the related work to our research. The previous work done allied to cloud outages is described in this chapter.

Chapter 4 discusses the current business situation for cloud services. It includes details about how the cloud services are deployed and what are the important factors considered. The description about inputs for our model and where this model can stand in the current business situations is added in this chapter.

Survey was conducted as a part of this thesis to help understand the various challenges faced by consumers. Survey results obtained are from the consumer point of view, since the respondents of this survey were consumers. Survey results support my idea of assessing risk for cloud outages. It helped me to understand, how exactly consumers react to cloud outages and how severe is the impact of cloud outages. The steps taken for this survey, results and responses of this survey are pronounced in Chapter 5. There are several service providers available for a single cloud service, which provides similar functions to the consumer. However, selecting the right service provider is a complex decision for the consumer. Selecting the right service directly help to reduce the risk of cloud service.

Chapter 6 presents implementation of a well-known mathematical model to select a right provider for a single cloud service. This model considers requirement, cloud providers, service level parameters, and cost all as inputs.

Chapter 7 introduces the term risk assessment. Our model considers all the inputs and assesses the risk of cloud service based on the inputs provided.

Chapter 8 gives the conclusion for the complete thesis, we describe the benefits, assumptions as well as challenges for my formal model to reduce the risk of cloud outages.

Chapter 9 provides all the references and cited articles

There are two Appendixes A in this thesis. One is the historic data in a tabular format used to predict the risk of cloud outages. Historic Data is assumed, which thoroughly represents actual data in real scenarios. The second Appendix B includes the IRB approval confirmation. It was a requirement to conduct the survey.

1.4 Major Thesis Contributions

In this section we talk about major thesis contributions. We introduce the concern of cloud outage and reasons for cloud outages. Survey was conducted for this research which provided vital results. The survey results support our claim that there is a need of risk assessment for cloud outages. Survey results show us that proactive approach and solution to calculate the risk of cloud outages will help to reduce the impact and risk of cloud outages to a good range. Therefore, we provide a direct solution to calculate and control the risk of cloud outages by implementing a well-known mathematical model to select the right provider and further we analyze the risk of important service level parameters of a cloud service. Risk assessment is implemented by introducing a valuable term Value At Risk (VAR) and considering historic data for a single service. The final results show the worst possible values and probability of occurrence of cloud outage for the service. This thesis is a contribution to help businesses reduce the risk of cloud outages by introducing verifiable SLA's which consider downtime and risk as most important parameters, which will bring visibility for both cloud providers and cloud consumers. This will enhance the basis for negotiation using other important terms like cost and quality of service in SLA with risk of cloud outages

CHAPTER 2: BACKGROUND

2.1 Overview

Cloud computing is increasingly becoming the rule and not an exception, everyone has different opinions about cloud and one of the ways to quantify the true value of cloud as mentioned in this article [23] is that cloud brings benefits to the industry these benefits are hard to calculate. For example in the cloud, via PaaS one can deploy application and increase capacity much easier and more quickly than one could if one had to manage the hardware directly. For example if there is a seasonal Christmas retailer, who requires excessive computing capacity during the month of December, its much faster to scale up shopping application in the cloud, which can store more data compared to earlier months of the year. In such a situation, an application would have taken weeks and months to just enable this same service for more capacity. Since cloud is always pay as you go service, cost is also a complex term to consider here. Generally, cost of a service is for the functionalities of the applications. But, when we think of cloud outages (downtime) is not considered for cost of a service or in SLA. More specifically there is a concern on how to find cost about slowdowns, or glitches, performance, unavailability for cloud services [17]

Cloud computing concerns clearly indicate there is a hidden cost of downtime while using cloud services. A survey was conducted in the article [17], which shows the major concerns of cloud services from management point of view are as shown in the Table 1

Table 1: Top Cloud Computing Concerns

Top Cloud Computing Concerns	Percentages
1. Poor end user experience due to performance bottlenecks	64%
2. The impact of poor performance on brand perception and customer loyalty	51%
3. Loss of revenue due to poor availability, performance or troubleshooting	44%
4. Increased cost of resolving problems in a more complex environment	35%
5. Increased effort required to manage vendors and SLA's	23%

The vital issue that we consider in our research here is that downtime is never considered for calculation of cost in SLAs. Availability is the only way to calculate the cost for computing a cloud service; there is no vibrant method to calculate the amount of risk a consumer is investing in cloud services. Few cloud providers provide some amount as a reimbursement for the downtime of service but service unavailability can result substantial impact on business functions at the consumer end, which is obviously higher than just the reimbursement amount provided by the cloud service providers. Our thesis will consider this issue where consumer gets frustrated while waiting for the service to be offered. Our approach here is to have a proactive solution to this situation. If the consumer knew in advance that such unavailability was inevitable and knew the estimated time duration, risk for loss of revenue well in advance, it would help consumer to take corrective measures well in advance before selecting the cloud service provider. A cloud service is well defined by the service level parameters. Our model will consider key performance indicators of a service as the parameters to be measured, in order to know the risk of cloud outages well in advance. The service level for these key parameters gives a clear picture whether the service is performing at its best or not.

2.2 Detailed Study

Here, the research will reveal the causes of cloud outages supported by online Resources [7] the author describes the reasons for top most reported cloud outages in the year 2012. There were 22 publicly reported cloud outages and 6 outages due to hurricane sandy during the same year. The information about length of these outages is displayed in Table 2. The idea here is to discuss that outages those that can be due to any reason and length of time for which outages occur is not known in advance. The length of time varies to a very large extend. When we consider measuring the impact of cloud outages, it vastly depends on the downtime length of a service.

Table 2: Length for Cloud Outages

Percentage	Outage Length
18.2%	<1 hour
31.8%	1-4 hours
18.2%	4-8 hours
22.7%	8-12 hours
9.1%	>12 hours

In one of the recent studies [20] authors specify the fundamentals of the risk involved with data storage because most of the leading organizations consider moving data out of their own data centers and into the cloud. Authors report on success for cloud storage providers can present a significant risk to customers; namely, it becomes very expensive to switch storage providers. Authors argue here that striping user data across multiple providers can allow customers to avoid vendor lock-in, reduce the cost of switching providers, and better tolerate provider outages or failures. The study [14] was conducted for 172 cloud outage security vulnerability incidents. Among the known threats, insecure interfaces and APIs, data loss or leakage and hardware failure constitute 25% of the threats and account for 64% of all cloud vulnerability security incidents. These were most frequently seen threats. But these incidents contribute only to 75% of the known causes for the cloud outages. This study [14] also shows that there are 25% of unknown causes for cloud outages. See Figure 1

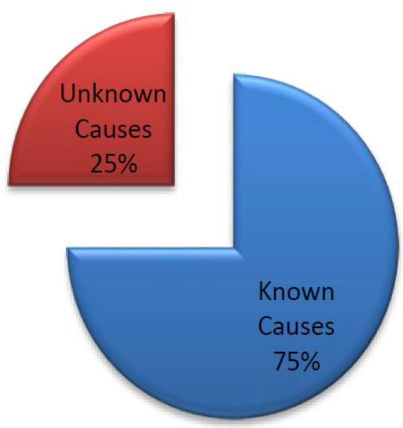

Figure 1: Causes for Cloud Outages

The study reported in [3] shows that there is a need for separate security SLAs for the business; security is important factor to consider in SLA according to this study. The security is another quality parameter, which if measured well in advance can help to reduce the risk of cloud outages due to unsecure cloud services. The study [14] reveals that there are several unknown causes for cloud outages and this passes unknown risk with cloud services. Both consumers and providers are clueless about such unknown risk, since it is not mentioned in any SLA. Often these SLAs are driven only by the availability and service is sold on demand of availability. Availability is the biggest concern while considering cloud outages. When the percentage of availability mentioned in a SLA is 99.999% this means there can be a downtime of 26 minutes per month and a 5 hours and 15 minutes of downtime per year. Even if a cloud service performs fairly satisfactory throughout the year, still a single outage of 5 hours can result in significant loss. Table 3 shows the percentages and downtime of availability. Total downtime is mentioned in HH:MM:SS format.

Table 3: Availability Percentages and Downtime

Availability	Per Day	Per Month	Per Year
99.999%	00:00:00:4	00:00:26	00:05:15
99.99%	00:00:08	00:04:22	00:52:35
99:9%	00:01:26	00:43:49	08:45:56
99%	00:14:23	07:18:17	87:39:29

We already discussed availability and security as important service level parameters for cloud services. Let us now discuss the possibilities of cloud outage if cloud service is not 100% reliable. Data storage, data retrieval, data redundancy are important for cloud service which offer data functionalities. We can say a service is reliable, only when all data is survived during failure. Data synchronization is important to consider reliability of data. As reported in [1] ACID Atomicity, Consistency, Isolation, Durability (ACID) properties are essential for transactional reliability and immediate consistency. This means reliability of service is an important measurement to consider while selecting a service. However, consumers do not know such measurements of parameters. If we consider end user point of view, downtime is a downtime whether it is due to availability issues or reliability of a service or security of a service.

Consumers are unaware of the measurements of the service level parameters before as well as after occurrence of an outage. Measurement of the quality of a service with service level parameters is complex as well as difficult due to these reasons we discuss here. One reason is cloud services are offered in various ways like Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Additionally, these services are offered in varying price plans. For example, a well-known cloud service provider Amazon provides different service types for developers, businesses, and enterprise and there are more than thousands of different pricing plans. Cost is important to consumers as well as providers. Providers claim the best service level parameters like 99.99% and 99.999% of availability to sell their service and consumers cannot measure these parameters in advance. This creates a misunderstanding between a cloud provider and a cloud consumer, as there is no reflection of risk to both providers and consumers. Few service providers in the industry consider planned downtime and unplanned downtime. Planned downtime is mentioned in an SLA to avoid later confusions, when cloud outages occur. Planned downtime is usually the result of having to do some sort of software maintenance or release process, which is usually mentioned in the SLA. Still planned downtime does not solve the concern of cloud outages here. Unplanned downtime is not visible to both cloud consumer and provider while signing a service level agreement. Consumers have the right to be aware of risk involved due to unplanned downtime, so that they can prepare to back up their critical data and save the essential data of their customers or end users.

It will be insightful for cloud consumers to have the ability to verify SLA parameters by themselves. Verifying SLA independently will reduce the dependency of cloud consumers on the providers. This justifies that cloud consumer will acquire control over the service, which will help them to take proactive actions before cloud outage occurs. For cloud services in banking, health care industry such verifiable SLA's can be so beneficial, to save the data from the critical applications and reduce the impact of loss due to cloud outages.

Our model includes a verification action by consumer to assess the risk of cloud outage well in advance before moving the critical applications to the cloud services.

CHAPTER 3: RELATED WORK

Studies and research is done to improve features of cloud services, in order to minimize the impact of cloud outages. The whitepaper “An introduction to designing reliable cloud services” the author David Bills [5] provides fault injection as one of the solution to improve the reliability of a cloud service. Fault injection can be viewed as using software that is designed to break other software. For teams that design and deploy cloud services, it is software designed and written by the team to cripple the service in a deliberate and programmatic way. It is mainly used with stress testing and is widely considered an important part of developing robust software. When using fault injection on a service that is already deployed, organizations validate strategies for minimizing the impact of unexpected outages. Cloud providers can discover unexpected results that are generated by the service by fault injection method. Fault injection helps to get information to the service provider about the service such as whether the service is functioning as expected or whether unexpected faults occur under load.

Reliability is important to consider as discussed earlier. A cloud service with good reliability helps to reduce the impact for failure. According to [5] and IEEE, “Reliability in a design engineering discipline means applying scientific knowledge to assure that a system will perform its intended function for the required duration within a given environment, including the ability to test and support the system through its total lifecycle". For software, this paper [5] and IEEE defines reliability as “the probability of failure- free software operation for a specified period of time in a specified environment”. The author mentions that some degree of failure is inevitable (cannot be prevented). I consider this idea as the basis for my thesis. In my model I will, consider measuring unknown risk of cloud outage. The risk is calculated before finalizing SLA with a cloud provider.

The author David, Bills [5] indicates, there are cost tradeoffs associated with reliability strategies and that should be considered in order to implement a service with sufficient reliability at optimal cost. For our proposed model we take into account, most important service level parameters, which also include reliability.

“Measured service is an essential characteristic; where there should be control and optimization of resource usage” according to NIST [20]. This gives transparency for both the provider and consumer of the utilized service. Our proposed model, considers this risk as a calculated term to include in SLA, where consumer and provider can have full transparency about the resource usage as well as risk involved due to unplanned downtime or a cloud outage.

Service level monitoring is the key considerations for continued monitoring and availability of cloud services. There are tools available to monitor the cloud services. One of the software available with features for Service Level Monitoring (SLM) is uptime software [11] Uptime software is the creator of uptime, the complete IT dashboard for watching over servers, applications, networks and IT services.

Service level monitoring tools provide important data, which act as measuring performance data to know if the service is performing according to the service levels mentioned in the SLA. It has five key steps according to this paper [11]. They are get quick wins, determine metrics that matter to the business, set realistic and achievable SLA targets, move beyond the rigid and complex framework solutions, which is a win-win situation for both providers and consumers. Setting realistic SLA targets is very important to avoid the risk of failure or unavailability. Hence, it is very important to set clear service levels and also refining them over time.

"Service level management is described as monitoring and management of service quality using a set of key performance indicators" according to [11]. For our model, we considered clear key performance indicators, with clear pre-defined expectations. SLM then compares the actual performance with pre-defined expectations. One of the initial and most important steps mentioned in this paper [11] is about base lining the service quality. For organizations that are just entering in SLM, it is encouraged that they monitor current service levels and baseline the quality of service that they will provide. This enables them to gauge whether they can meet the expectations of the business units with existing resources or it will need to make added investments in infrastructure to achieve expected results. By describing the success stories about uptime software, the paper [11] illustrates that SLM has created a demand for new tools and solutions that advanced the process by keeping track of service levels over time and analyzing historical service level trends. IT organizations can use SLA monitoring and reporting tools to predict and prevent problem before they impact business users. Enhanced service level management solutions enable the providers to quickly set the SLA service levels. Intelligent alerting notifies the users if SLA is at risk.

Such information is useful to get hold of potential issues and quickly drill down to service level objectives to determine which components of infrastructure are causing SLA at risk. Enhanced service level management with tools like uptime software increases visibility. It gives immediate results unlike other tools, which take months and years to deploy. Predictability to remove risk is another important feature of such SLM tools. Responsiveness with such tools is important for alerting the risk of cloud outage, reporting with clear graphs and data help business managers to monitor service measures and impact on infrastructure. Whitepaper [10] does the potential analysis for the SaaS service in order to do functional and economic analysis for evaluation. It introduces a term called Potential Adoption Index (PAI) is the weighted score calculated which could be used to compare two different SaaS solutions. If PAI exceeds 2.5 in the calculation it means there is a positive balance between economic components, characteristics, risk factors, and benefits of cloud computing in the adoption of the analyzed SaaS solution for the company

CHAPTER 4: CURRENT BUSINESS IN THE CLOUD

4.1.Cloud Business

In this chapter we consider important business scenarios and SLA.We also illustrate how it relates to cloud outages. Usually cloud services are offered in following types

1. Web applications that cater to diverse users across the internet and demand fast response times
2. Enterprise applications that cater to different business units across the world and require large amounts of secure, reliable data transfer and high availability (99.999%).
3. Scientific applications that need raw CPU or enterprises that perform batch processing.

The first two types of applications need systems that depend on in our daily life and these need to dependable and long lived. Dependable means that service offered for such functions should be reliable, available and secure. However, our daily life brings a lot of changes and so our requirements change for these cloud services. These changes in requirements consequently necessitate change in priorities for quality parameters for users. For example, for few situations reliability can be more important for a service compared to security. Consider a festival time for a Diwali shopping service or a Christmas shopping website. In such cases, availability of a service becomes more important for that festive season

When a cloud provider offers this service, the consumer has to pay according to the requirements of the service that both cloud consumer and provider have agreed to. This means consumer will have to pay more cost if the cloud provider provides a service, which is more reliable. If a consumer is paying for more reliable service, clearly there should be a trust that cloud outage will not occur or the % of occurrence should be to its minimum. Clearly if we consider calculating the risk of cloud outage due to low reliable service, we need to consider requirements for reliability by the consumer.

For current as well as future cloud services one of the vital things to consider is standardization mention here few of the standards and models used in current industry to improve the quality of cloud services, several standards discussed in [9] are listed below.

- Cloud Security Alliance (CSA)
- Distributed management task force (DMTF)
- Storage Networking Industry Association (SNIA)
- Open Grid Forum (OGF)
- Open Cloud Consortium (OCC)
- Organization for the advancement of structured Information Standards (OASIS)
- TM Forum
- Internet Engineering Task Force (IETF)
- International Telecommunications Union (ITU)
- European Telecommunications Standard Institute (ETSI)
- Object Management Group (OMG)

The cloud standards also discusses about cloud management. For example provisioning, metering and billing, security, privacy, quality of service and identity all are part of cloud management for any type of service. SLA is the most important contract to mention while talking about standardization. All SLA's cannot be same, since the services differ to very large extend, but following the standard and correct guidelines for building an SLA is important. SLA standardization brings more visibility among the cloud actors a provider, consumer and other actors. Preparing a right SLA which consider all the possibilities of risk of cloud service and brings visibility is a good SLA according to our research.

4.2. Service Level Agreements

The process of preparing SLA for a cloud service should never be rushed, it is important to consider what service guarantees consumers expect. In the paper [19] author discusses that rushing the process of negotiating terms and conditions doesn't give enough time for the parties to understand each other's expectations particularly when each party has a different perception for what a certain terminology stands for. It is also important to consider the details about each term and condition that a consumer and provider should agree upon. These terms and conditions may differ to little extend with different services. Terminology used should be common with provider and consumer. Cloud provider should evaluate its relationships and SLA's with vendors, enterprise data centers, network providers, and content providers. In this paper [19] the author provides the best practices and how the SLA's can be standardized. All these factors of misunderstanding, rushed process and unclear terminology and requirements can add to the risk of these cloud services going unavailable or not meeting the expectations. But these risks are never calculated in the migration process and at several occurrences these risks are categorized as unknown risks. Author for this well written paper [19] illustrates the six testing types consumer should use to test web services before a service is made public. TM forum standards mentioned above defines SLAs as expectations among two or more parties regarding service quality priorities, and responsibilities. The other standard cloud standards customer council views cloud SLA's as written expectations for service between cloud consumers and providers. SLA's are not a one way solution for example: the cloud service provider should not impose decisions about how things should be done, particularly when the other party the cloud consumer has different expectations about how the SLA should be formulated. It doesn't have the inputs from all pertinent parties that must be involved. Other exceptions to include in an SLA are failure, network issues, denial of service, scheduled maintenance. A right SLA can bring clear objectives, clear service features, terms, which will directly be helpful to reduce the misunderstandings and also reduce the chance of failure of a service. We consider these factors to be important for this thesis because our proposed model is to reduce the risk of cloud outage since the start of a service, to migration and until the service actually starts at the consumer side.. All SLA's are about service guarantees regardless the type of service provided. Penalties are imposed if service guarantees are not met, but the clause of exit should be the important part of SLA. For example, the penalties provided are always mainly for the time when service was unavailable but the consumers are not paid for other revenue loss or reputation loss due to unavailable services. Hence, the exit clause should clear mention when a consumer can exit from the contract. For example, if the loss of revenue is too high, a consumer should have the right to exit the service and move to a different provider in that case. Consumers should be allowed to get the services tested and service should provide testing report which include response time, throughput, elasticity (internally scaling, agility). Such reports will be helpful to calculate the risk of cloud outages. We show how historic data of a service can help to calculate the risk of cloud outages. Historic data can be one year old or even 6 months old data.

Other important considerations in an SLA are cloud metrics, which mention user threshold levels, resources threshold levels, quality service parameters threshold levels. It is important to know who is going to set these threshold levels for service, it depends on the control variables assigned to the users and providers, for example: a SaaS end user doesn't set any threshold levels. The only control the user has is to access the application from either the provider or the PaaS developer from a desktop or a mobile or a laptop. The threshold level access may differ according to type of services. If a SaaS service fails, the end user may be unaware of what the actual cause of failure since he may not have all the access for the SaaS service, on the other hand IaaS user may have more control over the service. So IaaS user may be able to figure out the exact reason for a failure much quicker when compared to SaaS end user. The SLA for a SaaS is not as complex as the SLA for a PaaS.

The penalties mentioned should be very clear while negotiation as they may highly impact the SLA process. For example: a certain cloud provider may provide 20 % rebate of service fees for cloud service downtime exceeding one hour while another provider might provide 25% rebate of service fees for cloud service downtime exceeding just about half an hour. Both the partners in an SLA should be clear about what the penalty is and when to impose.

Identifying the correct members in an SLA is first and most important steps to consider. According to NIST the five important members to be included are:

- Cloud consumer
- Cloud provider
- Cloud carrier
- Cloud broker
- Cloud auditor

There are few drawbacks here while a considering cloud actor one of, which is many a times consumers do not know whether these actors have one to one or one to many relation. There can be another drawback here, consider a cloud service which is very small and may not need vendors or brokers to be included. In such case still considering other actors may increase the complexity. Also, when the service is unavailable even for few seconds or minutes, it may have impact to more number of users if more actors are considered in an SLA. The SLA service levels and policies should always be evaluated against the current business processes and situations. It is also important that SLA should follow the current business strategy and policy. All these factors contribute to making a good SLA contract. An outage can be of different types and one of which is due to unclear consumer expectations. A good SLA contract with clear expectations directly helps to reduce the risk of outages.

Scaling of cost with quality of service via SLA is always a challenge; Let us understand here, how a service level agreement will define cost and other features. This webpage [6] defines what are the types of risks involved with cloud computing and how to deal with them. It rightly says," Fear of failure must never be a reason for not to try something", There is no denying that cloud computing has certain concerns, but cloud services have benefits, as well. It is always better to recognize beforehand some risks with cloud computing. This is the rationale as to why we are considering our risk assessment model to stand exactly at a point before the SLA contract is actually signed. One of the main reasons of cloud outages is the cloud provider not meeting the requirements of quality standards or service levels for the consumer. Quality standards required for a cloud service should also match the cost requirements for the cloud service. For example, the provider may impose higher cost for 99.999% availability compared to 95% availability. On the other hand, risk involved with 95% availability would also be high compared to 99.999% availability. Hence, scaling the cost with the quality levels and risk of outages is a complex part to consider in our model. Today all types of organizations, such as startup companies and large organizations are moving to cloud services and providing cloud services. This is because cloud computing provides a plethora of benefits. Consumers considering the use of cloud based services or planning to invest in cloud services need to exercise caution in evaluating small cloud based companies because quality is becoming harder to assess and measure. It is becoming important to model service quality in the cloud. It is important that service quality be measured for each requirement by consumer. Therefore, in our thesis we will consider measuring the actual versus committed service quality values of these service level parameters and complete an analysis of outage risks. Figure 2 describes where the formal model will stand in the current business.

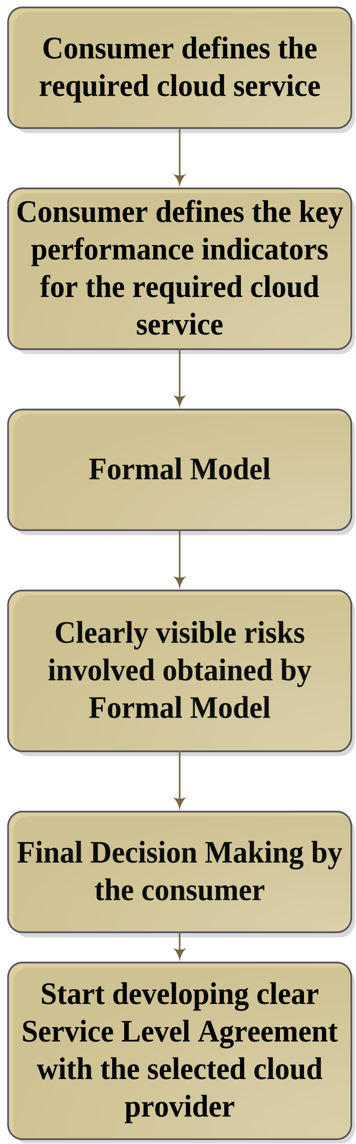

Figure 2: Formal Model in Current Business

CHAPTER 5: DESIGNING AND CONDUCTING SURVEY

We reached at a point where we understood the important area of concern both cloud providers and consumers are facing. We were certain that there is a need for risk assessment for cloud outages. However, there was no provision to this proposed idea of risk assessment. Therefore, in order to move our research in the right direction, we decided to conduct a survey for this research. The reason for leading this survey was to know the need of risk assessment from the consumer point of view. To complete our research successfully; it became important to know whether consumers will accept such idea of risk assessment before signing a SLA. If they accepted, how helpful would such model be to the consumers? The finest alternative for getting the reactions from consumers was by conducting this survey in an accurate manner.

5.1.Survey Details

The decision taken was to conduct this survey by creating a simple and useful questionnaire. While creating this questionnaire it was important all necessary information required to support our model was acquired. Survey results helped us to validate whether, our proposed model can really be helpful to consumers. Earlier, our research revealed that selecting right provider, prioritizing service level parameters and scaling the quality of service with cost help to reduce the unknown risk. Measuring quality parameters will bring visibility of risk. Therefore, all this reviewed research helped us to create a well-defined questionnaire

The idea here to allow consumers make independent decisions to reduce the risk of cloud outage, therefore we decided that the respondents of this survey will cloud consumers. The next important step after creating the questionnaire was to gain the IRB approval, which is attached in the Appendix B. Survey Monkey tool helped us to create this questionnaire and estimated time to take this survey by each respondent was of 5-10 minutes. The targeted number of respondents was about 60-65.

The web link was passed to various respondents via email campaign. In total, we received 59 responses from cloud consumers. The respondent's belonged to different organizations few of which were developers who use PAAS cloud service and others as managers, test engineers and solution architects. Other respondents belonged to big consulting organizations those who frequently use cloud services for their clients from various industry sectors.

5.2.Survey Results

In this section we describe each question of the survey and provide the results. Survey monkey did not have a feature of quantitative analysis. Therefore, we did the analysis manually by assigning a numeric value to each response option for a question. This gave us the information about the most predicted response by consumers in future. This clearly helped us to validate our formal model.

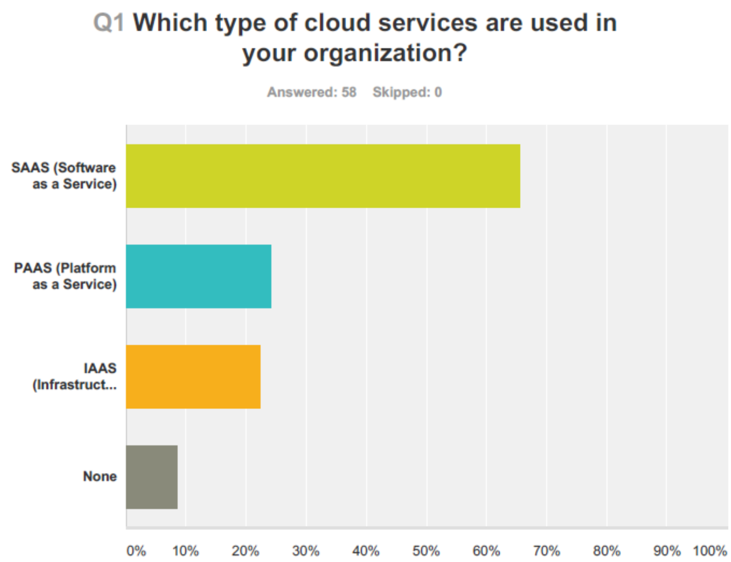

Figure 3: Survey Responses for Question 1

We received in total 58 responses for question 1. SaaS is most widely used cloud service. Almost 66% of respondents mention that SaaS is used in their organization as shown in Figure 3. However, our model does not depend on the type of service. We consider this result to show that our model can be used in organizations, which use all types of cloud services. we will not go into the detail of numeric analysis for this question as it is more generic question and results of this question will not change much in our proposed idea.

Numeric analysis will be conducted for all other questions of the survey. We consider following values to organize the quantitative analysis

1. Survey Question
2. Total number of respondents for each question
3. Numeric value is assigned to each option of response in the ascending order (1-4)
4. Total number of responses for each option

We multiply the assigned numeric value of each option with the number of responses for that option. This will give us the weightage value for each response. The final result for each question will be calculated sum of weightage/total number of respondents. We will then check where the final result falls in the numeric range. The will provide us the most predicted response option for each question when more number of respondents taking this survey.

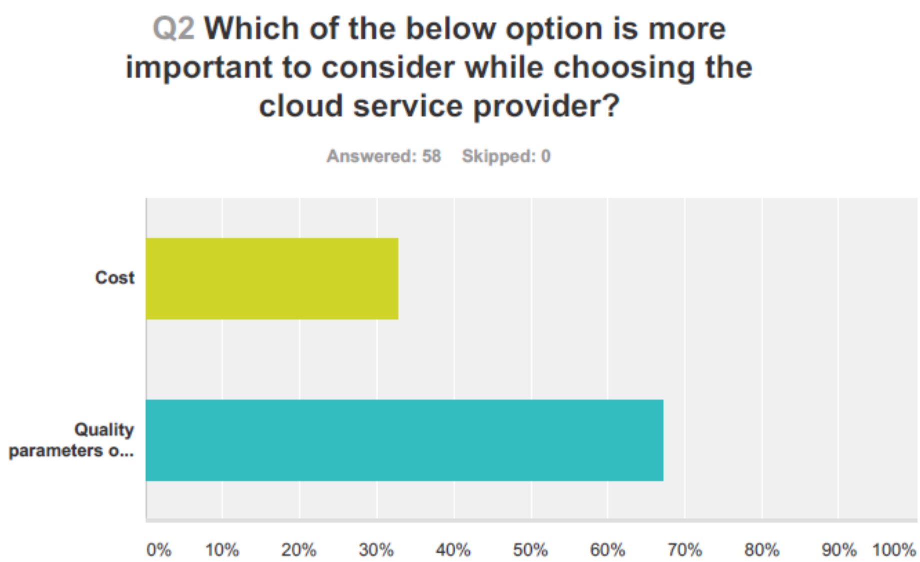

Figure 4. Survey Responses for Question 2

In Question 2 as shown in Figure 4, we ask the consumers if cost is important for their cloud service or quality parameters are important. Our earlier research revealed that, sometime cost becomes more important for consumers, which result in selecting a low quality cloud service. The survey results show that quality parameters are more important to the consumers because critical functions of their business directly depend on quality of cloud service. The quantitative analysis to predict the future responses for this question is provided in Table 4.

Table 4: Survey Responses for Question 2

Assigned numeric value	Response options	Number of Responses	Weightage of each response
1	Cost	19	19
2	Quality parameters	39	78
		Sum=	97
		Final Result=	97/58=1.67

The result is 1.67 which means, cost is not always important and quality parameters are also not always important. But, since the value of final result falls in the range, it means sometime cloud consumers give importance to cost and at certain occurrences quality parameters are more important. Our model will consider such situation, where priorities of service level parameters will change according to different business scenarios.

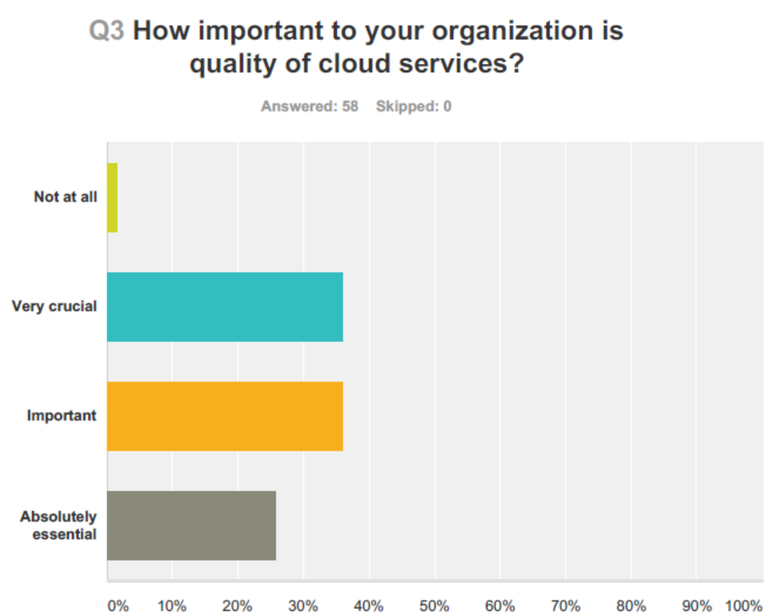

Figure 5: Survey Responses for Question 3'

Table 5: Quantitative analysis for Question 3

Assigned numeric value	Response options	Number of responses	Weightage for each response
1	Not at all	1	1
2	Very crucial	21	42
3	Important	21	63
4	Absolutely essential	15	60
		Sum	166
		Final Result	2.862

The final result is 2.862 as shown in Figure 5 and Table 5 this means, the quality of cloud services is important for cloud consumers.

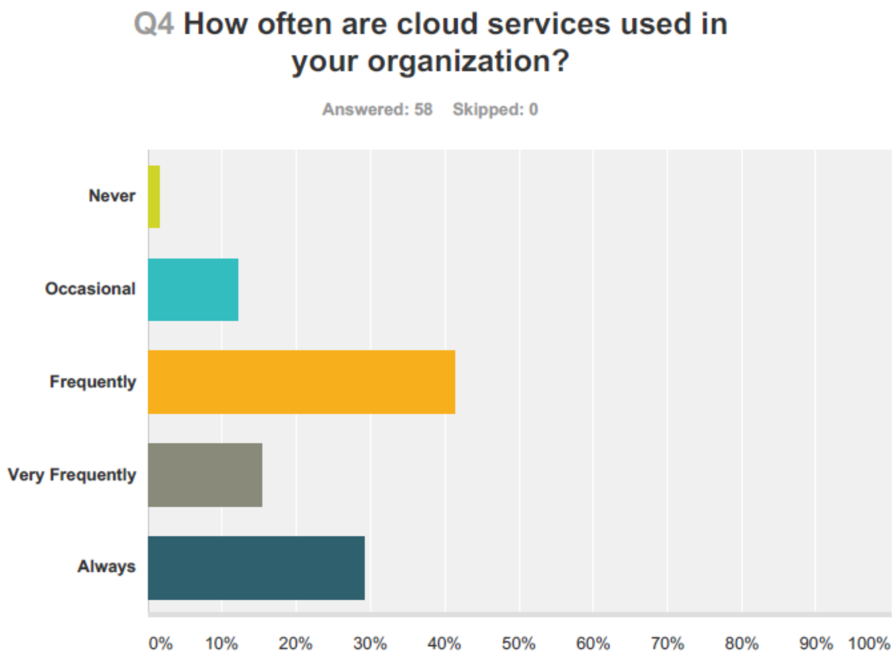

Figure 6: Survey Question 4

Table 6: Quantitative Analysis for Question 4

Assigned numeric value	**Response options**	**Number of responses**	**Weightage for each response**
1	Never	1	1
2	Occasional	7	14
3	Frequently	24	72
4	Very frequently	9	36
5	Always	17	85
		Sum	**208**
		Final Result	**3.586**

The final result for Question 4 is 3.586. This shows us that Cloud services are very frequently used in organizations today. It means critical applications of consumers; highly depend on availability, reliability and security of these cloud services.

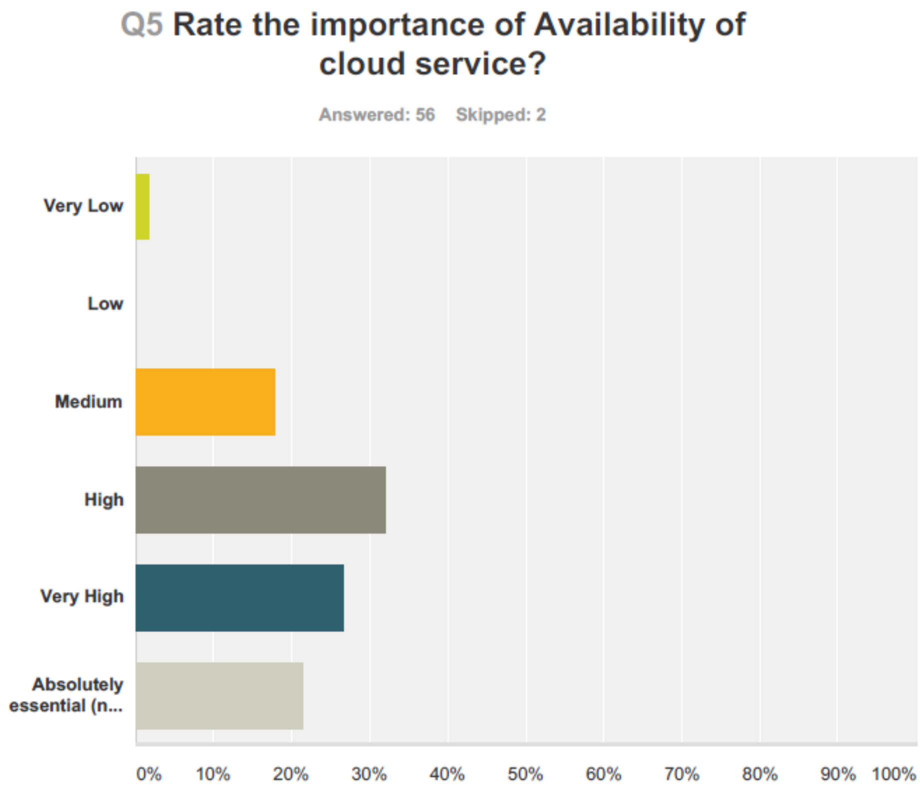

Figure 7: Survey Question 5

Table 7: Quantitative Analysis for Question 5

Assigned numeric value	Response options	Number of responses	Weightage for each response
1	Very Low	1	1
2	Low	0	0
3	Medium	10	30
4	High	18	72
5	Very High	15	75
6	Absolutely Essential	12	72
		Sum	**250**
		Final Result	**4.464**

The result for Question 5 is 4.464 as shown in Table 7. This mean the importance of availability is high to consider the right cloud service according to consumers. Therefore, we consider Availability as important parameter in our model.

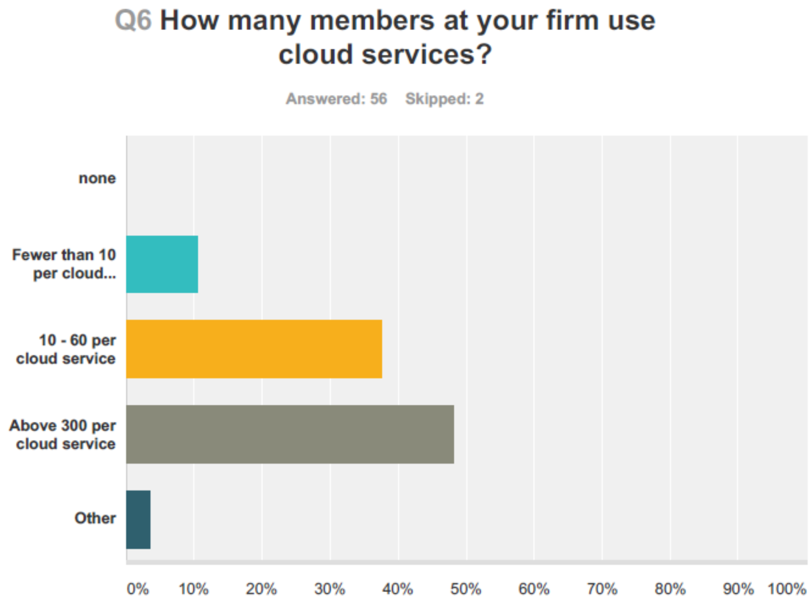

Figure 8: Survey Question 6

Table 8: Quantitative Analysis for Question 6

Assigned numeric value	Response options	Number of responses	Weightage for each response
1	None	0	0
2	Fewer than 10 per cloud service	6	12
3	10-60 per cloud service	21	63
4	Above 300 per cloud service	27	108
5	other	2	10
		Sum=	**193**
		Final Result=	**3.446**

The final result for Question 6 is 3.446. This shows us that sometimes the number of users for a single cloud service exceeds above 60 and above 300. This gives us the information that number of end users depending on a single cloud service is more. A cloud outage of even few minutes can bring significant loss of customer loyalty is such situations.

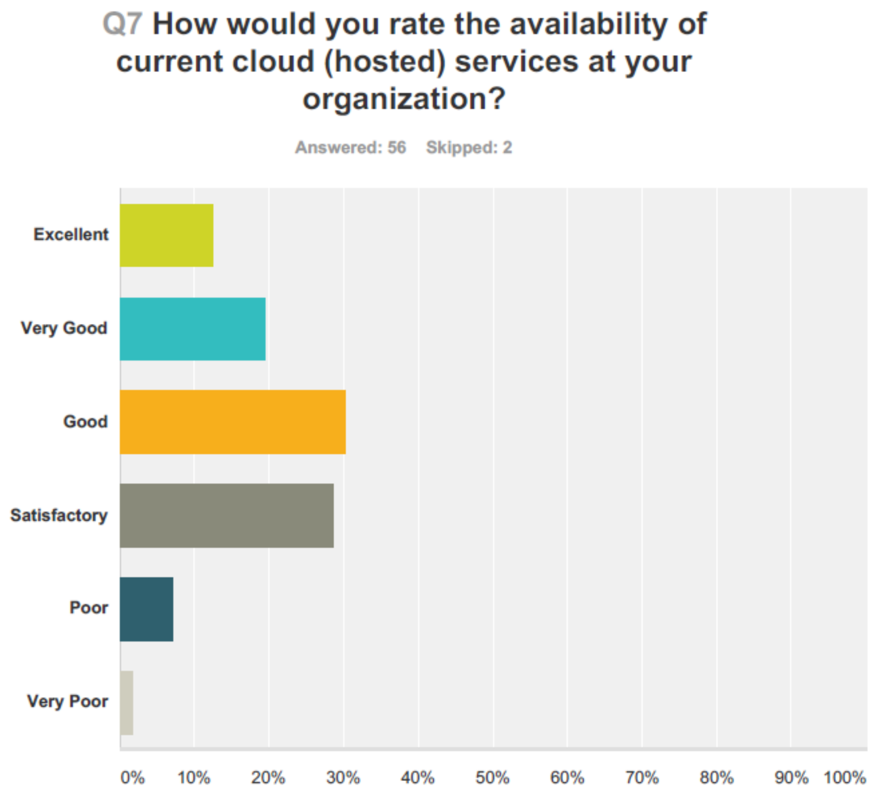

Figure 9: Survey Question 7

Table 9: Quantitative Analysis for Question 7

Assigned numeric value	**Response options**	**Number of responses**	**Weightage for each response**
1	Very Poor	1	1
2	Poor	4	8
3	Satisfactory	16	48
4	Good	17	68
5	Very good	11	55
6	Excellent	7	42
		Sum=	**222**
		Final Result=	**3.96**

As the result value in Table 7 is 3.96. It means, consumers say that availability of current cloud services at their organization is satisfactory, but not excellent.

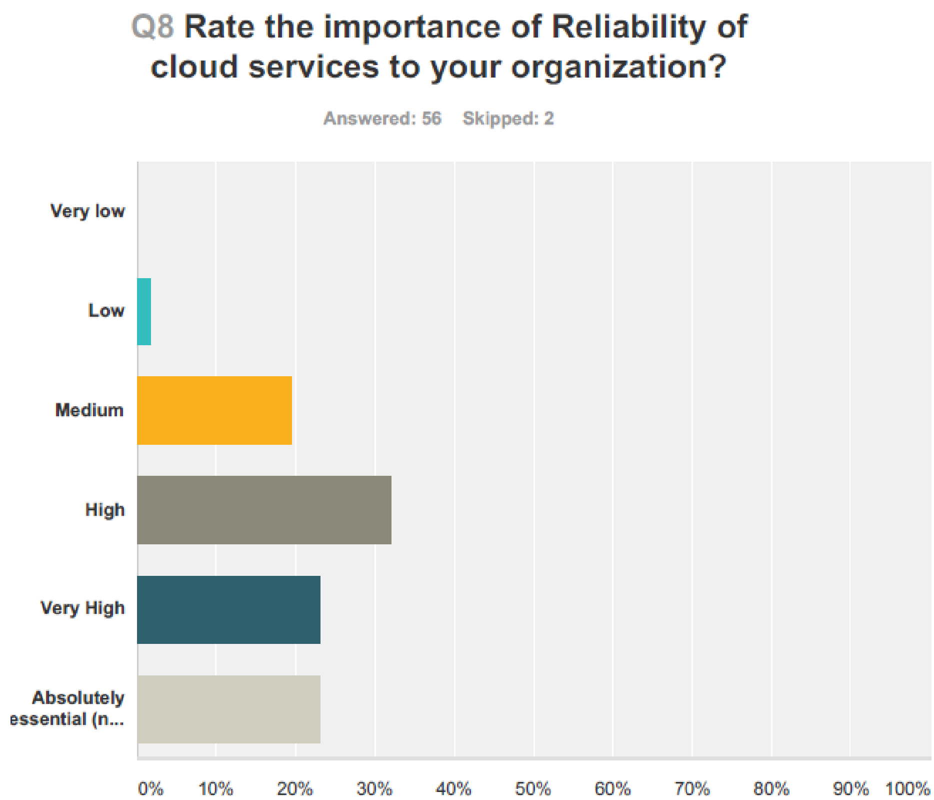

Figure 10: Survey Question 8

Table 10: Quantitative Analysis for Question 8

Assigned numeric value	Response options	Number of responses	Weightage for each response
1	Very Low	0	0
2	Low	1	2
3	Medium	11	33
4	High	18	72
5	Very High	13	65
6	Absolutely Essential	13	78
		Sum=	**250**
		Final Result=	**4.464**

The final result in the Table 10 shows the value as 4.464. This means reliability is an highly important characteristic to select a right cloud service for the consumer. Reliability is considered in the model as a parameter for which the committed values and actual values will be measured.

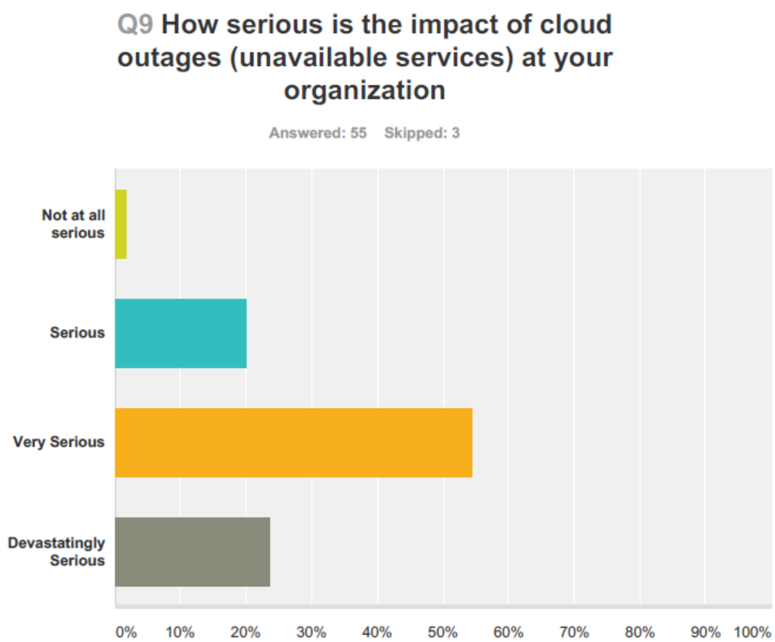

Figure 11: Survey Question 9

Table 11: Quantitative Analysis for Question 9

Assigned numeric value	**Response options**	**Number of responses**	**Weightage for each response**
1	Not at all serious	1	1
2	Serious	11	22
3	Very serious	30	90
4	Devastatingly serious	13	52
		Sum=	**165**
		Final Result=	**3**

Table 11 shows final result value as 3, which reveal that the impact of cloud outages in current industry is very serious according to consumers.

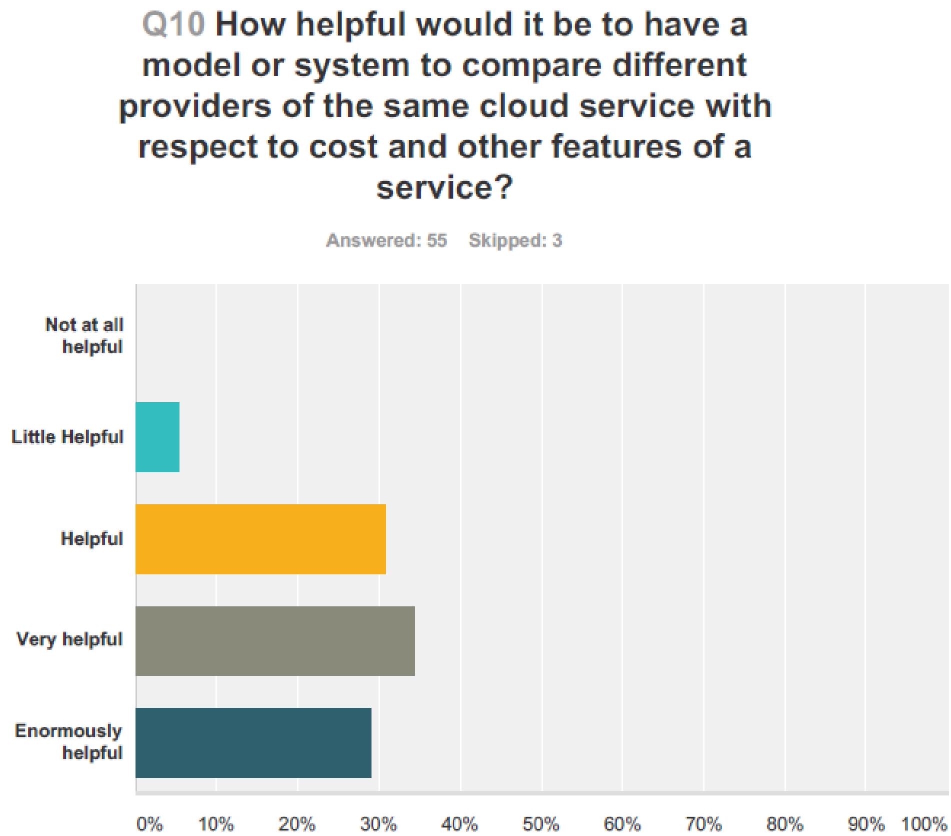

Figure 12: Survey Question 10

Survey Question 10, as shown in Figure 12**,** is we ask the consumers how helpful will be our proposed idea of a model. The survey results for this question clearly support our idea that such system or model will be helpful to consumers. This validates our idea very strongly.

Table 12: Quantitative Analysis for Question 10

Assigned numeric value	Response options	Number of responses	Weightage for each response
1	Not at all Helpful	0	0
2	Little Helpful	3	6
3	Helpful	17	51
4	Very Helpful	19	76
5	Enormously Helpful	16	80
		Sum=	**213**
		Final Result=	**3.872727273**

The results in Table 12 show the value as 3.87. This means our model which will select the right provider will be very helpful to consumers.

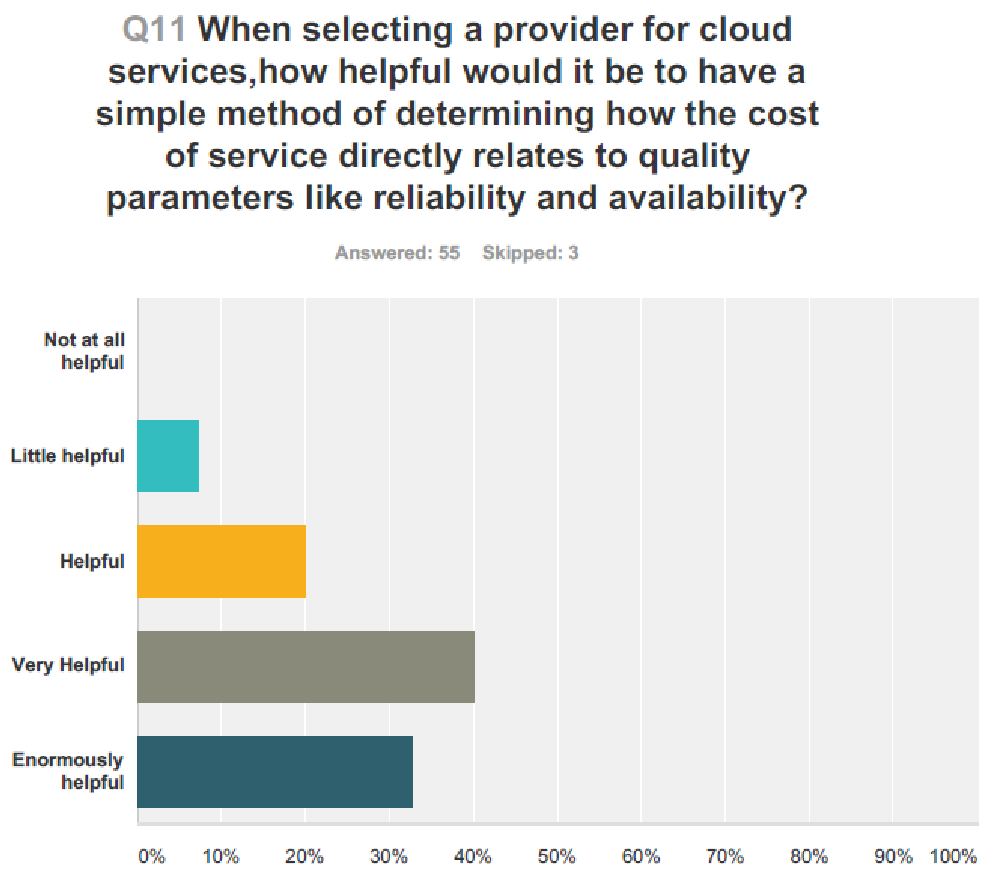

Figure 13: Survey Question 11

In Question 11, as shown in Figure 13 we check that how do consumers consider scaling of service parameters with cost. They are unaware how to measure service parameters, that is why we ask this question to gain the information. If the service A is more reliable than service B, than consumer may pay more cost for service A. But, still the problem of cloud outages will exist, when consumer pays more cost for Service A.

Table 13: Quantitative analysis for Question 11

Assigned numeric value	Response options	Number of responses	Weightage for each response
1	Not at all Helpful	0	0
2	Little Helpful	4	8
3	Helpful	11	33
4	Very Helpful	22	88
5	Enormously Helpful	18	90
		Sum=	**219**
		Final Result=	**3.98**

As the Table 13 show that final result is 3.98. This clearly means that our system will be helpful to consumers, if our model or a system provides the information for measuring quality with cost.

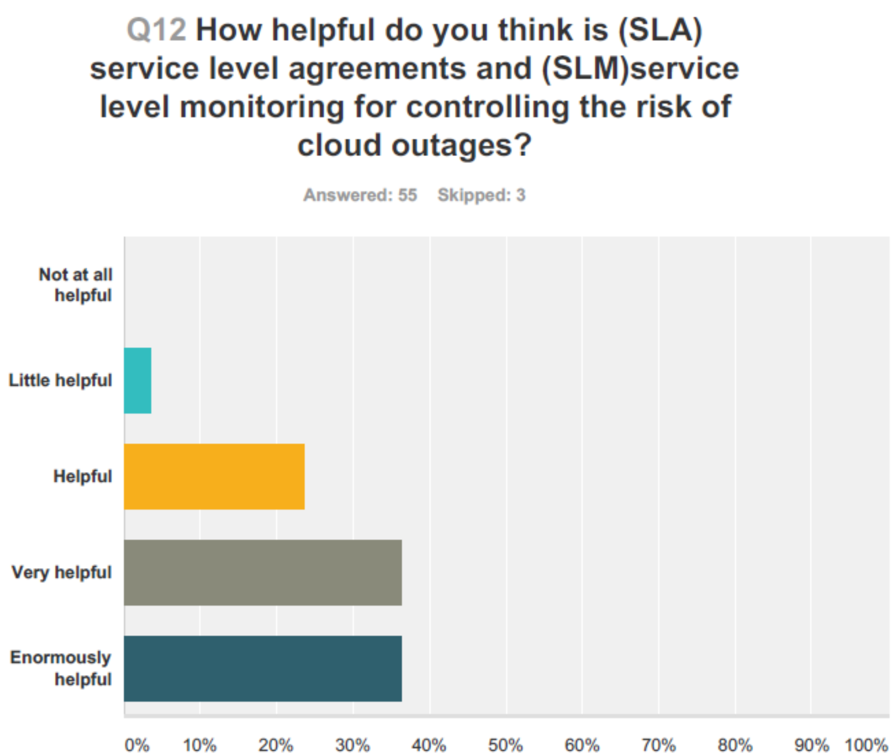

Figure 14: Survey Question 12

Service level monitoring has become integral part of maintaining cloud services. In `Question 12 as shown in Figure 14 we ask the consumers if SLM can be helpful to control the risk of cloud outages. The quantitative analysis is shown in

Table 14: Quantitative Analysis for Question 12

Assigned numeric value	**Response options**	**Number of responses**	**Weightage for each response**
1	Not at all Helpful	0	0
2	Little Helpful	2	4
3	Helpful	13	39
4	Very Helpful	20	80
5	Enormously Helpful	20	100
		Sum=	**223**
		Final Result=	**4.054**

The final results in Table 14 show as 4.054. This means Service Level Monitoring is considered very important and is used very often in cloud industry today. This supports are method of model, where we consider historic data of a service which is collected by conducting monitoring of service previously.

It became important for our research, to understand what the important service level parameters according to consumers are and how they prioritize them. Results for Question 13, as shown in Figure 15 help us to know the important parameters according to consumers. Quantitative analysis for not required for Question 13 as the important service parameters may change according to type of service. We consider the priority of these parameters according to consumer point of view in our model.

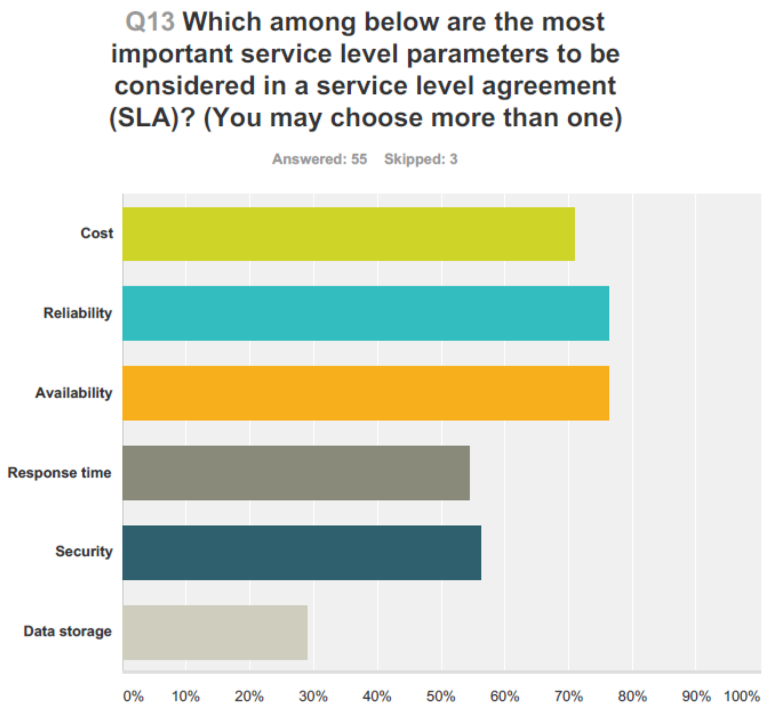

Figure 15: Survey Question 13

This response shows us that all these parameters are important to consider in a cloud service according to consumers as shown in Figure 15**.** I will consider all combinations of priorities in my model to select the right provider with such priorities of service parameters.

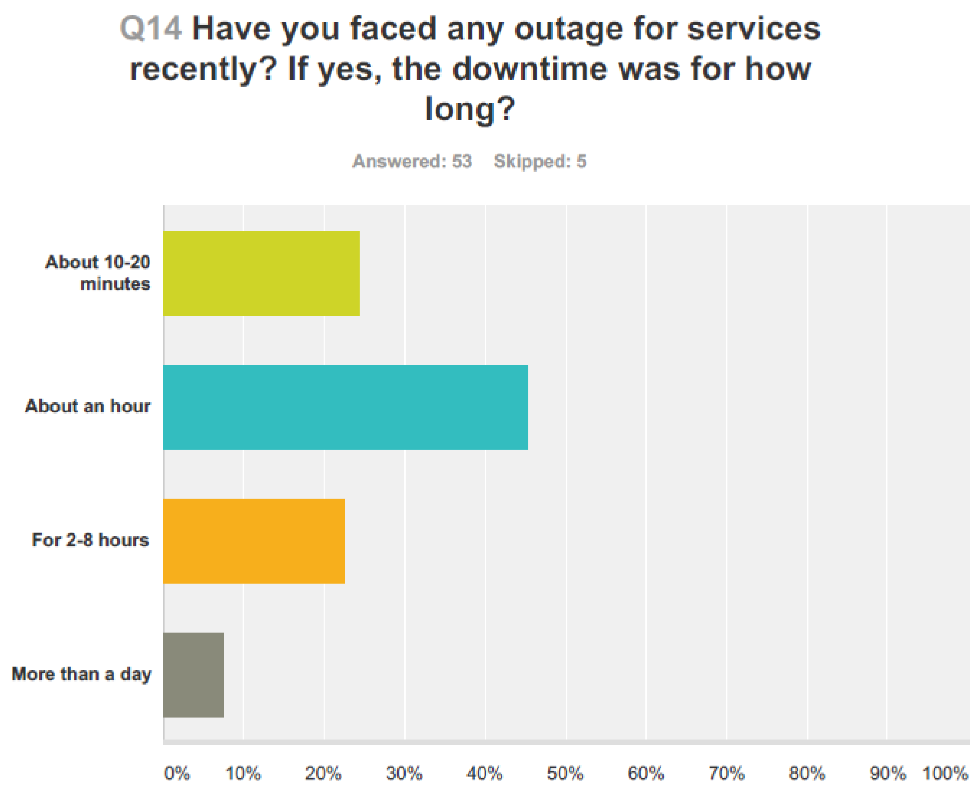

Figure 16: Survey Question 14

There are several recent cloud outages faced by industry today. We get the information about these in Question 14 as shown in Figure 16

Table 15: Quantitative Analysis for Question 14

Assigned numeric value	Response options	Number of responses	Weightage for each response
1	About 10-20 minutes	13	0
2	About an hour	24	4
3	For 2-8 hours	12	39
4	More than a day	4	80
		Sum=	**123**
		Final Result=	**2.320**

As shown in Table 15, the final result for Question 14 is 2.320. This means, that consumers have faced the downtime of cloud service for about an hour on a monthly basis. This is definitely the area of concern that we talking about in this thesis.

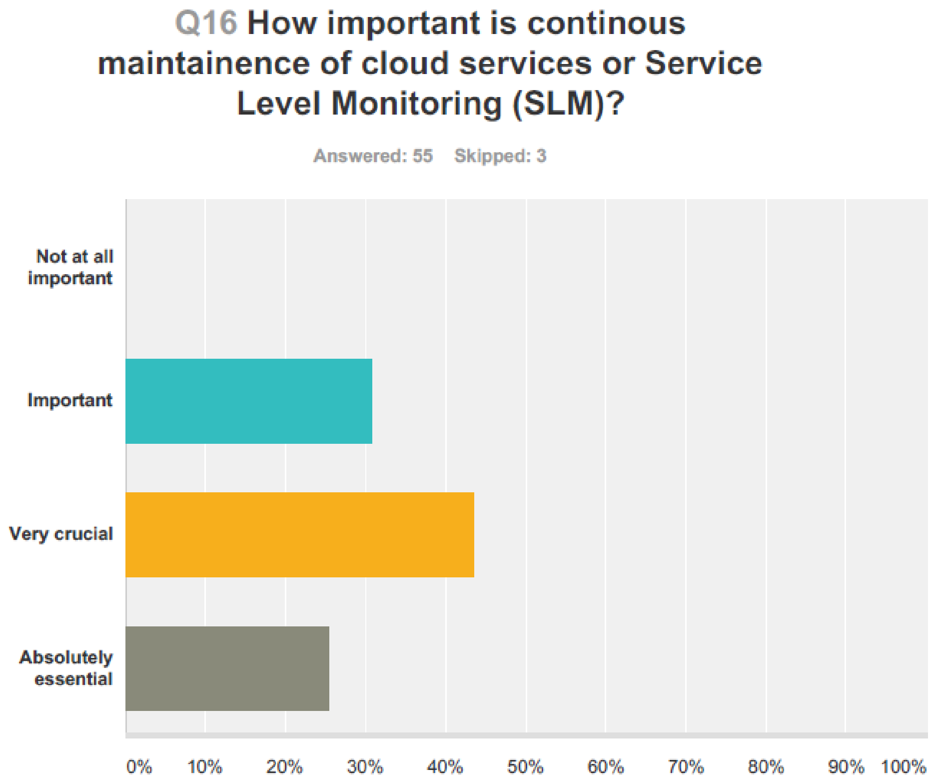

Figure 17: Survey Question 16

The Figure 17 show that service level monitoring is very crucial to cloud consumers. Let calculate the final result according to quantitative analysis in Table 16

Table 16: Quantitative Analysis for question 16

Assigned numeric value	Response options	Number of responses	Weightage for each response
1	Not at all important	3	3
2	Important	11	22
3	Very crucial	24	72
4	Absolutely essential	17	68
		Sum=	**165**
		Final Result=	**3**

The final result for Question 16 is 3 as shown in Table 16**.** This means, continuous maintenance of a service is important for consumer organizations. Even though, service performs today, but tomorrow it may not perform well. Therefore, continuous maintenance is essential as suggested by our survey results

#	Responses
1	Continuous monitoring is important for cloud services. Choosing the right performance parameters is very important.
2	Calculating risk ahead of time, before an outage is a good idea.
3	NA
4	Good survey. . No addition required. .
5	Nice survey
6	Cloud services needs to be more robust in terms of security and reliability.
7	Just to reiterate, i think crucial factors in deciding vendor is availability,security & cost. It is also helpful to have an idea of what underlying technologies they are using so that we can be hopeful of them meeting their SLAs.
8	Everybody has cloud outages as no cloud implementation is 100 percent reliable. So, it is very important to calculate the risk involved during migrating the application to cloud and during the cloud outages. So, it seems to be a great topic for thesis which calculates the risk involved in cloud outage along with the cost scaling to select appropriate service provider.
9	Security is the first point in storing data on cloud, so consider that always :)
10	Currently when we are using the cloud services, with our software helping users issue Legal notices and data storage, it is absolutely important that we maintain confidentiality and there is no loss of data at any given point
11	Good topic to have the opinions of people
12	cloud services is the present and going to expand in future. The less downtime it has, the less customer is impacted.

Figure 18: Additional comments for Consumers

Figure 18, shows the additional comments provided by the consumers. We see consumers have no tolerance for data loss in comment 10. Security is important to consumers as in comment 9. Verifying SLA can be helpful as mentioned in comment 7. Comment 2 says it is a good idea to assess the risk well in advance. Choosing a right service with right quality parameters is important. We conclude that survey results are definitely supporting our idea of choosing the right provider and assessing the risk of cloud outages, well in advance.

CHAPTER 6: SELECT THE RIGHT SERVICE PROVIDER

In Chapter 5, we discussed the survey results, which clearly showed that our idea will be supported by the consumers. Here, we implement the idea of selecting the right cloud service provider. Service Level parameter values of a service, determine if the service is a low quality service or a high quality service. For this we consider defining these service parameters for this model. Application availability is the amount of overall time the application is expected to be operational accounting for planned downtime for software upgrades, tuning, maintenance and support. Reliability is the amount of time the application is operational without unexpected outages or downtime due to underlying infrastructure such as hardware failure, installation, power outages, and other issues. Different service providers provide varying price plans for planned downtime and unplanned downtime. So, calculating this risk of outage directly depends on the service provider selected. For this model, which selects the right provider we consider calculating the risk of an outage for each eligible service provider.

The output of this model will be a detailed report that consumer will use to analyze the risk and make an educated decision. I consider different set of priorities by a consumer for each service parameter.

This model is retrieved from one of the conference proceedings [12]. After implementing this mathematical model [12] which selects the right provider, risk is assessed for each eligible cloud provider to get the final results.

6.1. Modified Weighted Product Model

The mathematical model adopted for our model is very well known model which is used to resolve complex decisions. Decision making is complex specifically when more number of parameter’s are to be considered. As detailed earlier in Chapter 1, reliability, availability, security or any other service level parameter can become a reason for cloud outage. Hence, all these parameters are important to be considered for my model. Our model has multiple steps, and breakdown structure.

The mathematical model [12] used for this model is existing weighted product model, which helps in decision making paradox situations. Risk will be calculated after ranking the various service providers for a particular requirement. Before moving ahead to the proposed model, let us understand how weighted product mathematical model is useful to our model. This formal model should give an output which can be analyzed very easily by consumers. For example: A consumer may want to analyze which provider is best among the list and meets all the requirements of a service. Requirements of service are defined in terms of parameters like availability, reliability. In real situations, consumer may want to select the service with the minimum risk of cloud outage provided at optimum cost. Our model will help decision making to meet all these requirements. This means all these factors comprehensively may help making an informative decision to the consumer while selecting the service. Weighted product model will be used to select the right provider and calculations of risk of cloud outage will be performed using additional formulas and data. One of the conference proceedings [16] from the journal “Decision Support Systems” describes various methods for decision making in complex situations.

There are three methods of decision making described in this paper [12]

1. Determining the relevant criteria and alternatives

2. Attaching numerical measures to the relative importance of the criteria and to the impacts of the alternatives on these criteria.
3. Processing the numerical values to determine a ranking of each alternative.

Our model will implement the third method from above. The various alternatives to be considered are service level parameters. A consumer can choose a service based on the requirement and priority for service parameters. For example: For a Consumer C1 security may be much more important compared to response time. For a Consumer C2 availability can be more important than security.

As described by author Evangelos Triantaphyllou and Stuart H. Mann [16] the weighted sum model (WSM) is commonly used approach especially in single dimensional problems. If there are M alternatives and N criteria then, the best alternative is the one that satisfies in the maximization case the following expression

Equation 1 : Weighted Sum Model

$$A *_{WSM=max_i} \sum_{i=0}^{n} a_{ij} w_j \text{ for i =1,23,.......,m}$$

Where A (WSM score) = the WSM score of the best alternative, N= the number of criteria, $a_{i\,j}$ = the actual value of the i^{th} alternative in terms of the j^{th} criterion, w_j = the weight of importance of the j^{th} criterion. The assumption that governs this mathematical model is the additive utility assumption. That is to say that total value of each alternative is equal to the sum of products given as above expression in (1). In single dimensional cases where all the units are the same (example dollars, feet, seconds) the WSM can be used without difficulty. We implement the mathematical model that is a modified version of weighted product model. Weighted product model (WPM) is very similar to Weighted Sum Model (WSM). The main difference is that instead of addition in the model there is multiplication. Each alternative is compared with the others by multiplying a number of ratios, one for each criterion. Each ratio is raised to the power equivalent to the relative weight of the corresponding criterion. In general, in order to compare the alternatives A_k and A_L the following product has to be calculated using Equation 2

Equation 2: Comparing alternatives

$$R\ (A_K/A_L) = \prod_{j=1}^{N} (a_{Kj} / a_{Lj})^{wj}$$

Where N = the number of criteria, $a_{i\,j}$ = the actual value of the ith alternative in terms of the jth criterion, w_j = the weight of importance of the jth criterion. If the term R (A_k/A_l) is greater than or equal to one, then it indicates that the alternative A_k is more desirable than the alternative A_L. The best alternative is the one that is better than or at least equal to all the other alternatives. The WPM is sometimes called dimensionless analysis because its structure eliminates any units of measure. Thus, the WPM can be used in single dimensional and multi-dimensional decision making problems. One advantage over using WPM instead of WSM is that instead of actual values it can use relative ones.

This modified version is implemented in one of the international journal (19) related to selecting the right service provider using SLA.

SLA’s help a cloud consumer to choose the best cloud by matching the requirements with the services offered by clouds as mentioned in the service level agreements. However, SLA’s do not consider downtime and unplanned downtime is never mentioned in SLA. When service outages do occur providers offer reimbursement to customers for the cost of their services during the period of the outage. Providers are not inclined to pay penalties that would reimburse for loss of business revenue or costs consumers incur because of cloud outage. The response time, slowing down of a service, and downtime in a consumer organizations are just accepted as a fact of life. These SLA's sound pretty good at a 99.9% uptime, however 99.9% availability is a nine hours a year of downtime. So once critical business applications are considered, many users have very little tolerance for downtime before suffering a major adverse business impact or loss of revenue. In this light nine hours can be a lot. Referring to the examples of cloud outages in the year 2013 [18],even few hours of downtime can cause million dollars of loss of revenue depending on the size of the company and the business applications involved. Our formal model is to include calculating risk of cloud outage in SLA's. However this entire process of matching the requirements and calculating risk of cloud outage becomes quite complicated when performed manually by the cloud customer or a consumer. Also, there is increasing number of providers offering services with growing popularity of cloud services. If the requirements of the service and risk of cloud outage are not matched well to select the cloud provider, it may result in a business situation where consumer may take a wrong decision and risk critical applications while moving them to cloud service. The main purpose of our model is to match these service requirements. Our model will support to select the provider with the minimum risk of cloud outage well in advance, before moving the critical applications to cloud. It may also be possible that the selected best provider for a requirement have high risk of cloud outage. Our model will support and alert the consumer about the high value of risk. Hence keeping this in mind we provide a framework that removes the burden of risk of cloud outage from the customer. The model in [12] will be used to select the best cloud provider by comparing different clouds on the basis of service they offer and on the basis of user requirements and priorities. After the ranking is obtained for various service providers, historic data will be considered for each of these providers and risk value of outage due to each service level parameter will be calculated. As discussed in Chapter 2 cloud outage can occur due to any reason. Few of the reasons are availability service levels not met as required and mentioned in SLA or security service levels not met as in SLA, reliability service levels not met as in SLA. It is possible that service goes offline even service levels for one of the quality parameters go low. Our model will give the actual Values At Risk for each of these parameters.

In actual business scenarios cloud consumer may not know the infrastructure and network provider details for the cloud provider. While making a decision to move to cloud services, a consumer and a provider depend to a strong extend on a vital contract document called SLA. For this model, I assume that the consumer is very clear with the requirements in term of service level parameters. Priorities and cost for these important service level parameters should also be known well to the consumer. We assume that requirements, priorites and cost is very clear to the consumer and we create tables for these based on our assumption.

As mentioned we will implement modified version of Weighted Product Model (WPM) to select the right provider. Our model will consider following service level parameters. In real scenarios choosing the service parameters will depend highly on the type of service required by consumer.

- Availability
- Reliability
- Security
- Response Time
- Data Storage
- Cost of service per month

As implemented in the paper (19) following tables will be considered in this well-defined model to select the right provider. We assume the data for these tables. The data is representation of the actual data in tangible scenarios.

- Requirement Table
- Priority Table
- Cloud Provider Table

We reiterate the above mentioned WPM (Weighted Product Model) to illustrate how this mathematical model fits for cloud services.

Equation 3: Weighted Product Model

$$P (C_K/C_L) = \prod_n (C_{Kj} / C_{Lj})^{wj} \text{ for } K, L = 1, 2, 3 \ldots\ldots\ldots\ldots m$$

In the Equation 3: Weighted Product Model C_K and C_L are considered as two clouds. More specifically C_K and C_L are two different cloud providers for the same service. The purpose of implementing this model is to compare two different cloud providers C_K and C_L and rank them for a particular requirement.

Consider there are total m clouds and the ratio of all these m clouds is calculated. The ratio of two clouds is calculated by taking the product of ratios of each parameter. For example, if there are 3 parameters than

(C_{K1}/C_{L1}) * (C_{K2}/C_{L2})*(C_{K3}/C_{L3}) will be calculated in order to obtain final ratio $C_k/C_{L.}$ For our model there are 6 parameters. This would be done for each of the m cloud to know which one is the best. However, our approach will compare two clouds by taking the difference of their parameters instead of finding the ratios. As implemented in this paper (19) the difference is taken to compare two clouds. If P (Cloud A – Cloud B)>0, this means points of Cloud A are greater than Cloud B and thus Cloud A is better than Cloud B. We will now illustrate and fill data for all the tables and implement the mathematical model.

6.2. Requirements for Formal Model

We assume that consumer is clear about the required cloud service and the required service levels for parameters. Consumer is also clear about the requirements of business functions in his organization. Availability and reliability are important parameters according to survey results, so we consider all these parameters for this service. We consider response time as one of the other important parameter. Response time is the length of time taken for a system to react to a given tasks or event. In total we consider 6 parameters for the cloud service, Availability and Reliability have % as the unit. Security is calculated in hours. Response time is in seconds. data storage is GB and cost is in dollars. I assume that consumer, already knows what values for the requirement of these parameters are.

Table 17: Requirements by Cloud Consumer

Requirements	Availability	Reliability	Security	Response Time	Data Storage	Cost per month
R1	99%	94%	24	0.078	2500	$4,500
R2	99.90%	99.99%	23	0.098	3000	$3,800
R3	99.999%	99%	22	0.063	2800	$4,200
R4	99.99%	99.90%	24	0.055	2700	$3,500
R5	98%	99%	20	0.099	2000	$4,800
R6	99%	98%	21	0.098	2200	$4,300

In actual business scenarios these requirements can come by any cloud consumer willing to adopt a cloud service. This service can be any service (SaaS, PaaS or IaaS). Service parameters will differ according to type of service.

We already conducted survey to know the priorities by consumers in different organizations. We will include best priority set in Table 18 which is supported by our survey results. Security, reliability and availability, cost are to be ranked 1st in few of the combinations that we consider according to our survey results

Table 18: Priorities for Service Parameters by Consumer

Requirements	Availability	Reliability	Security	Response Time	Data Storage	Cost
R1	2nd	3rd	4th	6th	5th	1st
R2	3rd	2nd	1st	5th	6th	4th
R3	2nd	1st	3rd	4th	6th	5th
R4	1st	2nd	5th	6th	4th	3rd
R5	2nd	4th	1st	5th	3rd	6th
R6	3rd	1st	5th	6th	2nd	4th

A single cloud service is provided by so many different providers in the current cloud industry. For this model, we assume that cloud service required by consumer is provided by 6 cloud providers. Each cloud provider sells this service with different service values for parameters. The cloud provider Table 19 is assumed, this can be any providers in the market like

IBM, Amazon, Google, Salesforce or any small business cloud provider who provide the service required by the consumer. Cloud provider table is shown in Table 19

Table 19: Cloud Providers for Cloud Service Required by Consumer

Cloud Provider	Availability	Reliability	Security	Response Time	Data Storage	Cost
C1	99.990%	99%	24	0.077	2900	$4,000
C2	99.9999%	99.90%	24	0.036	2500	$4,500
C3	99.90%	99.99%	23	0.078	3100	$2,900
C4	99.9990%	99.09%	22	0.088	3000	$2,800
C5	99%	99.9990%	24	0.074	4000	$3,700
C6	99%	99%	23	0.099	4200	$3,300

We defined requirements, priorities, and cloud providers already in this chapter. All the required inputs are ready for implementation of Weighted Product Model to select the right cloud provider.

6.3.Implementation of Weighted Product Model (WPM)

The idea of implementing weighted product model is to compare various providers and find the most eligible provider for a single requirement. The committed values are the values of service parameters committed by cloud provider in the Table 19**.** The best cloud provider means the committed values of parameter by this provider, should match the entire requirement in Table 17 parameters required by the consumer for this service. As discussed earlier we will assign points to each provider. The provider with the best score will be most eligible provider for a single requirement. Before assigning points to each provider, the initial step is to find the eligible cloud providers from the list of 6 providers. In real scenario this step will involve finding the eligible cloud provider from several other providers. This step filters out, all the not eligible provider, making this model simpler to implement. For example: consider requirement 1 from Table 17 by single consumer and compare this requirement1 with the committed values by cloud provider C3 in Table 19. It is clearly shown that security requirement by consumer is 24 hours in requirement 1, but, the cloud provider C3 in Table 19 provides security for only 23 hours. Therefore, C3 is not eligible for requirement 1. It is important to **NOTE** here, that the cloud provider misses the eligibility criteria for consumer, even when single parameter service levels are not met as required. Similarly, cloud provider C4 is not eligible for requirement 1 because it provides the security only for 22 hours.

Now let us consider response time for requirement 1 and cloud provider amazon. In case of response time if the value is less, it means the service is better. Hence, response time with lesser value is much better service when compared with other provider. For requirement 1 the response time value is 0.078 second. This means any cloud provider providing service less than or equal to response time is eligible. Amazon provides the service at a response time of 0.099 second. Hence, Amazon is not eligible for requirement 1. We calculate such eligible cloud providers for all the requirements. Below is the result of eligible cloud providers.

For Requirement 1(R1): The eligible cloud providers are C1, C2, and C5

For Requirement 5(R5): the eligible cloud providers are C1, C2, C3, C4, C5,

And C6

For Requirement 6 (R6): The eligible cloud providers are C1, C3, C4, and C5

We will now calculate points for each provider using the mathematical model modified WPM where we take difference of provided values for each service level parameter. The values are cloud provider values for each service level parameters mentioned in the cloud provider table Point's calculation is as in the Equation 4

Equation 4: Point Calculation

Points ($Cloud_1$) = ($Cloud_1$ – $Cloud_1$) = (C_{11} - C_{11})*p1+ (C_{12} - C_{12})*p2 + (C_{13}- C_{13})*p3 ----- continued for 6 parameters

Points ($Cloud_2$) = ($Cloud_2$ – $Cloud_1$) = (C_{21} - C_{11})*p1+ (C_{22} - C_{12})*p2 + (C_{23}- C_{13})*p3------ continued for 6 parameters

Points ($Cloud_3$) = ($Cloud_3$ – $Cloud_1$) = (C_{31} - C_{11})*p1+ (C_{32} - C_{12})*p2 + (C_{33}- C_{13})*p3------ continued for 6 parameters

-

-

-

-

-

Points ($Cloud_N$) = ($Cloud_N$ – $Cloud_1$) = (C_{n1} - C_{11})*p1+ (C_{n2} - C_{12})*p2 + (C_{n3}- C_{13})*p3------ continued for 6 parameters.

The points obtained are arranged in descending order and ranks are found.

For our model there are 6 cloud providers and 6 parameters to be considered for each requirement. However for each requirement we have to consider only eligible cloud providers for ranking. Table shows the point calculations for Requirement. For requirement 1, the eligible cloud providers are C1, C2, and C5

Table 20: Point Calculations for Requirement 1

	Availability	**Reliability**	**Security**	**Response Time**	**Data Storage**	**Cost**
Points (C1) (C1-C1)	0	0	0	0	0	0
Points (C2) (C2-C1)	0.000198	0.027	0	0.246	-2000	-500
Points (C5) (C5 - C1)	-0.0198	0.02997	0	0.018	5500	300
Points (C1)= C1 - C2	-0.000198	-0.027	0	-0.246	2000	500
Points(C2)= (C2-C2)	0	0	0	0	0	0
Points (C5)= (C5-C2)	-0.019998	0.00297	0	-0.228	7500	800
Points (C1)= C1 - C5	0.0198	-0.02997	0	-0.018	-5500	-300
Points(C2)= (C2 - C5)	0.019998	-0.00297	0	0.228	-7500	-800
Points (C5)= (C5 - C5)	0	0	0	0	0	0

Let us understand how these values actually arrived. Points (C2) = C2 – C1= Here C2 –C1 means [(Availability provided by C2 in the cloud provider table) - (Availability provided by C1 in the cloud provider)]* Priority for requirement 1 in priority table

This is same as (99.9999%-99.990%) * 2 as we see in the cloud provider Table 19. This is equal to 0.0198% which is 0.000198 points for availability. In the same case C1- C2 will be negative same value as it will be calculated in the same way. Hence, value for C1 – C2 for availability is -0.000198. Negative number means the points will be deducted for the provider. In case of response time the lesser value is better hence, the cloud provider with the lesser response time for service should be given more points according to our mathematical model. Same is the case for cost. Lesser cost is better for consumer. So, whenever we calculate points for cost and response time we actually reverse the subtraction. Hence, in the row where we calculate

Points (C2) = C2 – C1 we actually calculate C1-C2 for cost and response time. Similarly we calculated points for all other parameters and all the eligible cloud providers. The final points calculated for each provider will be sum of all the points obtained for each parameter. All negative values will also be included in the sum to get the final points. The final resulted cloud provider matrix for requirement 1 is obtained in a matrix format. 0 values are C1- C1 points. Similarly, 2499.726 is C1- C2 and -2499.726 is C2-C1 points. Final matrix for requirement 1 is shown in Table 21

Table 21: Cloud Provider Matrix for Requirement 1

Cloud provider	C1	C2	C5
C1	0	2499.726	-5800.028
C2	-2499.726	0	-7499.754
C5	5800.028	7499.754	0

We now arrange the values in descending order. Ranking in all the three rows is same. C2 is first ranked, C1 as second and C5 as third. This gives us the ranking for cloud providers for Requirement 1.

We will proceed with similar calculations for other requirements. All cloud providers are eligible for Requirement 2. Therefore, the final matrix will compare all these providers.

Table 22: Point Calculation for Requirement 5

	Availability	Reliability	Security	Response Time	Data Storage	Cost
Points C1(C1-C1)	0	0	0	0	0	
Points (C1)(C1-C2)	-0.000198	-0.036	0	-0.205	1200	3000
Points C3 (C3-C1)	-0.0018	0.0396	-1	-0.005	600	6600
Points C4 (C4-C1)	0.00018	0.0036	-2	-0.055	300	7200
Points C5 (C5 -C1)	-0.0198	0.03996	0	0.015	3300	1800
Points C6 (C6 -C1)	-0.0198	0	-1	-0.11	3900	4200
Points C2 (C2 -C3)	0.001998	-0.0036	1	0.21	-1800	-9600
Points C2 (C2-C4)	0.0000	0.0324	2.0000	0.2600	-1500.0000	-10200.0
Points C3(C3-C4)	-0.00198	0.036	1	0.05	300	-600
Points C3(C3-C5)	0.018	-0.00036	-1	-0.02	-2700	4800
Points C3(C3-C6)	0.018	0.0396	0	0.105	-3300	2400
Points C2 (C2-C5)	0.019998	-0.00396	0	0.19	-4500	-4800
Points C2 (C2 -C6)	0.019998	0.036	1	0.315	-5100	-7200
Points C4(C4 -C5)	0.01998	-0.03636	-2	-0.07	-3000	5400
Points C4 (C4-C6)	0.01998	0.0036	-1	0.055	-3600	3000
Points C5(C5-C6)	0	0.03996	1	0.125	-600	-2400

We will sum all the points to result with the final Cloud Provider Matrix for Requirement 5 in Table 23

Table 23: Cloud Provider Matrix for Requirement 5

Cloud Provider	C1	C2	C3	C4	C5	C6
C1	0	4199.758	-7199.032	-7497.948	-5100.035	-8098.870
C2	-4199.758	0	-11398.79	-11697.707	-9299.793	-12298.62
C3	7199.0328	11398.791	0	-298.915	2098.997	-899.837
C4	7497.948	11697.707	298.915	0	2397.913	-600.921
C5	5100.035	9299.793	-2098.997	-2397.913	0	-2998.835
C6	8098.870	12298.629	899.837	600.921	2998.835	0

Now we arrange each row in Table 23 in descending order. The final ranking for cloud providers is obtained which is same in each row of Table 23.

C1- 2nd Rank

C2- 1st Rank

C3 – 4th Rank

C4- 5th Rank

C5 – 3rd Rank

C6 – 6th Rank

For Requirement 6 there are four eligible cloud providers.

Table 24: Point Calculation for Requirement 6

	Availability	Reliability	Security	Response Time	Data Storage	Cost
Points (C1) (C1 - C1)	0	0	0	0	0	0
Points (C3)(C3- C1)	-0.0027	0.0099	-5	-0.006	400	4400
Points (C4)(C4 - C1)	0.00027	0.0009	-10	-0.066	200	4800
Points (C5)(C5- C1)	-0.0297	0.00999	0	0.018	2200	1200
Points (C3) (C3-C4)	-0.00297	0.009	5	0.06	200	-400
Points (C3) (C3-C5)	0.027	-0.0001	-5	-0.024	-1800	3200
Points (C5)(C5- C4)	-0.02997	0.00909	10	0.084	2000	-3600

Final matrix obtained after sum of points for Requirement 6 is Table 25

Table 25: Final Cloud Provider Matrix for Requirement 6

Cloud provider	C1	C3	C4	C5
C1	0	-4795.0012	-4989.9352	-3399.9983
C3	4795.0012	0	-194.93397	1395.0029
C4	4989.93517	194.93397	0	1589.93688
C5	3399.99829	-1395.0029	-1589.9369	0

Ranking for Requirement 6 is

C1 - 1st Rank, C3 -3rd Rank, C4 -4th Rank,C5 - 2nd Rank.

Table 26: Final Ranking for Cloud Providers for all the requirements

R1	R2	R3	R4	R5	R6	Requirements
2nd rank	Not Eligible (Reliability and Cost)	Not Eligible (Availability, Response time)	Not Eligible (cost, response time)	2nd Rank	1st rank	**C1**
1st Rank	Not Eligible (Data Storage & Cost)	Not Eligible (Data Storage & Cost)	Not Eligible (Data Storage & Cost)	1st Rank	Not Eligible(Cost)	**C2**
Not Eligible (Security)	1st Rank	Not Eligible (Availability, Response time,)	Not Eligible (Availability, Response time, security)	4th Rank	3rd Rank	**C3**
Not Eligible (Security)	Not Eligible (Security)	Not Eligible (Availability, Response time)	Not Eligible (Reliability, security, Response time)	5th Rank	4th Rank	**C4**
3rd Rank	Not Eligible(Availability)	Not Eligible (Availability, Response time)	Not Eligible (Availability, Response time, cost)	3rd Rank	2nd Rank	**C5**
Not Eligible (Security & Response	Not Eligible(Availability ,response	Not Eligible (Availability, Response time)	Not Eligible (Availability, reliability,	6th Rank	Not Eligible (Response Time)	**C6**

The final ranking is obtained for all the requirements in Table 26. We introduced WPM and successfully implemented it in this chapter. The final ranking is shown in Table 26**.**Ranks the eligible cloud providers based on requirements, priorities and committed values of service levels for each service parameter by cloud providers. All important service parameters were considered to calculate the points for cloud provider. This will help to reduce the risk of cloud outage at the service levels. Final matrix of cloud providers was created for each requirement. The implemented mathematical model is beneficial for consumers. The model reduces the complexity of calculations to larger extend, because point calculation is performed only for eligible cloud providers. Not eligible cloud providers are filtered at the initial step. This is the advantage of using Weighted Product Model. The mathematical model is simple and easy to implement which ultimately make this model very valuable. The next step in this thesis is to assess the risk of cloud outage for each cloud provider ultimately leading us to the final results.

.

CHAPTER 7: RISK ASSESSMENT OF A CLOUD OUTAGE

In previous chapter WPM was successfully implemented, to rank the cloud providers for particular requirements. However to select the final service provider we still need to evaluate the unknown risk involved with the service. I introduce the risk assessment of cloud outage in this chapter.

We first present the term Value At Risk (VAR) which is more commonly used term in the financial industry. In financial industry, Value At Risk helps to measure amount of potential loss, probability of that amount of loss. For example, a financial firm may determine that it has a 5% one month Value At Risk of $100 million. Let us define this term here. “VAR is a statistical technique used to measure and quantify the level of financial risk within a firm or investment portfolio over a specific time frame”. VAR is used by risk managers to measure and control the level of risk which the firm undertakes.

We implement this term Value At Risk in our model, to calculate and control the risk of cloud outages by measuring service levels for parameters. We will now understand how this term can be used to control the risk of outages.

In order to assess the risk of cloud outage, I consider the results from the previous Chapter. Table 26 present us the ranked eligible cloud providers for each requirement. For requirement 2 the eligible cloud provider listed is Cloud Provider C3. C3 is the only eligible cloud provider for requirement 2, so it is ranked as 1st. Imagine this business scenario, where consumer with requirement 2 knows that cloud provider C3 is the most eligible provider for the service that consumer requires. Consumer has to decide whether C3 is the best provider and if the decision should be taken to move ahead with this provider. In this process, consumer is asking the cloud provider C3 what is the maximum risk of cloud outage associated with your service? This question may seem very direct and confusing to the cloud provider. It is a complex question, which do not have a direct answer. The cloud provider may not exactly know how much the maximum risk is. It definitely requires some statistical technique to answer this question. Cloud provider may or may not want to answer such question. Consumer will not receive the direct answer. The main purpose of our model is to find the answer to this question.

There are various factors on which the answer to this question will depend. One of the factors is type of service involved, pricing plans, and quality levels of service, infrastructure of this service, number of users involved, and many more. However, according to our formal model consumer with requirement 2 already know the requirements of the service and cloud provider C3 is already selected as most eligible provider for this requirement. The consumer now deserves to know whether risk is involved with the service, before moving ahead to sign SLA with the provider C3. Consumer does not know what will be the offered service levels for each parameter and how much is the risk involved due to poor availability or poor reliability, The whole idea here is to make the service level agreement verifiable for the consumer. More specifically, consumers do have the right to know answers to below listed questions and verify the SLA before signing it.

What is the maximum amount of downtime that can occur in a single day due to poor availability of cloud service?

What is the maximum amount of downtime that can occur due to poor reliability of cloud service?

What is the maximum amount of downtime that can occur in a single day due to poor security of cloud service?

What is the maximum amount of downtime that can occur due to poor response time or poor performance of service?

What is the maximum downtime that can occur due to insufficient data storage?

As shown in Table 3, even 99.9% availability can cause a downtime of about 8 hours a year. What happens if 8 hours of downtime occurs in a single day? There is a possibility of this worst day to occur when the service levels for availability are not met at all as mentioned in the requirements. This similar situation is applicable to other 4 service parameters reliability, security, data storage, and response time. The proposed idea here is know the probability of occurrence of such worst day. There can be few days of service when availability is more than expected and service meets all the requirements of parameters. There can be few other days when service levels for availability and other parameters is not met as expected. Since we are concerned to know the risk of cloud outage knowing the risk value during the worst day is important to complete my proposed idea. That will give the maximum value of risk with the service.

In order to calculate the maximum Value At Risk, we consider historic data. The assumption made here is that history is the best indicator to predict the future of a service. We consider past 6 months data as historic data of the service. Historic data is obtained by cloud provider. It is assumed data for 129 working days. It is shown in Appendix 1. Let us continue with the business situation, consumer requires historic data to evaluate the maximum risk. Provider will provide this data to the consumer. In real scenarios, the data can be collected for about a year. The more historic data will provide much accurate results. There are many service level monitoring tools in the market today which can be used to note the performance of cloud service in terms of service parameters. One of the earlier discussed software is Uptime software used for service monitoring. This data can also be acquired when performance testing or load testing is performed for the service, depending on the type of service. In this thesis we consider past 6 months data for cloud service by cloud provider C3 for requirement 2.

The requirement 2 from Table 17 is here

Requirement	**Availability**	**Reliability**	**Security**	**Response Time**	**Data Storage**	**Cost**
R2	99.90%	99.99%	23 hours	0.098 second	3000 GB	$3,800

We assume that cloud provider C3 provided the cloud service to some other provider starting from January 2013 to June 2013. Sometimes the service met the service levels as in the requirement 2 in the past six months. There were days when service went below the expected service levels

We calculate the rise and fall of this service value by using formula (x-(x-1))*100/(x-1) where x is the value for current day and x-1 is the service value for previous day. We calculate the rise and fall values for all the parameters except cost. Cost is already known to consumer and what amount consumer will pay for the service is already mentioned in the cloud provider Table 19.

Negative (-) value indicates, there was a fall in the performance value when compared to previous day. Rise or positive value, indicates there was an improvement in the performance when compared to previous day. All the values are calculated in Appendix 1.

From the historic data we easily determine the maximum fall in past six months for each service parameter. Highest fall for availability on a worst day is -7.923. To know the worst actual value for availability we subtract it from the committed value. The committed values by C3 can be found in Table 19. This means availability can go low to 91.977% and reliability can go low to 89.105%. All the values are shown in Table 27**.** Highest fall is determined from Appendix 1 for all the parameters and the worst possible values are calculated by subtracting higest fall values from committed values.

Table 27: Worst Possible Values

	Availability	**Reliability**	**Security**	**Response Time**	**Data Storage**
Highest fall of service levels	-7.923	-10.885	-19.048	4.067	-30
Worst Predicted Value = Committed value - highest fall	91.977	89.105	3.952	4.145	3070

The idea is clear that such worst levels for service parameters can occur on a single day or in a month or in a year. The next step is to know how frequently such worst service levels occurred during past six months. This will help us to predict the service levels for parameters in future. In order to know the frequency, histogram is the best idea. The frequency distribution in a histogram will help us to show how often each different value in a set of data occurs. We create the bin and frequencies for each parameter as shown in Table 28

Table 28: Bin and Frequencies for Service Parameters

Availability Bin	Availability Frequency	Reliability Bin	Reliability Frequency	Security Bin	Security Frequency	Response Time Bin	Response Time Frequency	Data Bin	Data Frequency
-8	0	-11	0	-20	0	-0.831	2	-30	4
-7.75	1	-10.75	3	-19.75	0	-0.581	8	-28.5	0
-7.5	0	-10.5	1	-19.5	0	-0.331	23	-27	0
-7.25	0	-10.25	0	-19.25	0	-0.081	24	-25.5	0
-7	0	-10	0	-19	2	0.169	23	-24	1
-6.75	0	-9.75	1	-18.75	0	0.419	16	-22.5	0
-6.5	0	-9.5	0	-18.5	0	0.669	6	-21	3
-6.25	0	-9.25	3	-18.25	0	0.919	3	-19.5	0

Availability bin	Availability Frequency	Reliability Bin	Reliability frequency	Security Bin	Security Frequency	Response Time Bin	Response Time Frequency	Data storage bin	Data Storage Frequency
-6	0	-9	0	-18	0	1.169	10	-18	0
-5.75	0	-8.75	0	-17.75	0	1.419	6	-16.5	2
-5.5	0	-8.5	0	-17.5	0	1.669	1	-15	1
-5.25	0	-8.25	1	-17.25	0	1.919	4	-13.5	0
-5	3	-8	2	-17	0	2.169	1	-12	1
-4.75	0	-7.75	4	-16.75	0	2.419	0	-10.5	0
-4.5	0	-7.5	0	-16.5	2	2.669	0	-9	3
-4.25	1	-7.25	0	-16.25	0	2.919	0	-7.5	0
-4	2	-7	0	-16	0	3.169	0	-6	8

Availability Bin	Availability Frequency
-3.75	0
-3.5	0
-3.25	0
-3	7
-2.75	2
-2.5	0
-2.25	0
-2	6
-1.75	5

Reliability Bin	Reliability Frequency
-6.75	0
-6.5	1
-6.25	1
-6	1
-5.75	1
-5.5	1
-5.25	0
-5	2
-4.75	0

Security Bin	Security Frequency
-15.75	0
-15.5	0
-15.25	0
-15	0
-14.75	0
-14.5	0
-14.25	2
-14	0
-13.75	0

Response Time Bin	Response Time Frequency
3.419	0
3.669	0
3.919	0
4.169	2

Data Storage Bin	Data Storage Frequency
-4.5	0
-3	18
-1.5	0
0	36
1.5	0
3	0
4.5	27
6	0
7.5	14

Availability Bin	Availability Frequency	Reliability Bin	Reliability Frequency	Security Bin	Security Frequency	Data Storage Bin	Data Storage Frequency
-1.5	0	-4.5	0	-13.5	2	9	2
-1.25	1	-4.25	0	-13.25	0	10.5	0
-1	17	-4	0	-13	1	12	1
-0.75	12	-3.75	0	-12.75	0	13.5	0
-0.5	0	-3.5	0	-12.5	6	15	0
-0.25	1	-3.25	0	-12.25	0	16.5	0
0	15	-3	1	-12	0	18	0
0.25	6	-2.75	2	-11.75	0	19.5	0
0.5	3	-2.5	4	-11.5	0	21	0

Availability Bin	Availability Frequency	Reliability Bin	Reliability Frequency	Security Bin	Security Frequency	Data Storage Bin	Data Storage Frequency
0.75	3	-2.25	3	-11.25	0	22.5	0
1	2	-2	2	-11	1	24	3
1.25	11	-1.75	2	-10.75	0	25.5	0
1.5	0	-1.5	2	-10.5	1	27	0
1.75	3	-1.25	6	-10.25	0	28.5	0
2	2	-1	2	-10	4	30	0
2.25	12	-0.75	5	-9.75	0	31.5	0
2.5	2	-0.5	2	-9.5	1	33	0
2.75	0	-0.25	5	-9.25	0	34.5	0

Availability Bin	Availability Frequency
3	0
3.25	0
3.5	0
3.75	0
4	0
4.25	4
4.5	2
4.75	3
5	0

Reliability Bin	Reliability Frequency
0	12
0.25	4
0.5	5
0.75	3
1	4
1.25	4
1.5	2
1.75	1
2	0

Security Bin	Security Frequency
-9	1
-8.75	0
-8.5	3
-8.25	3
-8	0
-7.75	0
-7.5	0
-7.25	0
-7	0

Data Storage Bin	Data Storage Frequency
36	0
37.5	0
39	0
40.5	0
42	0
43.5	4
45	0
46.5	0
48	1

Availability Bin	Availability Frequency	Reliability Bin	Reliability Frequency	Security Bin	Security Frequency
5.25	0	2.25	4	-6.75	0
5.5	1	2.5	1	-6.5	0
5.75	0	2.75	0	-6.25	0
6	0	3	1	-6	0
6.25	0	3.25	5	-5.75	2
6.5	1	3.5	0	-5.5	0
6.75	0	3.75	0	-5.25	0
7	0	4	2	-5	1
7.25	0	4.25	1	-4.75	4

Availability Bin	Availability Frequency	Reliability Bin	Reliability Frequency	Security Bin	Security Frequency
7.5	0	4.5	2	-4.5	6
7.75	0	4.75	1	-4.25	1
8	0	5	0	-4	1
8.25	0	5.25	0	-3.75	0
8.5	0	5.5	2	-3.5	0
8.75	0	5.75	0	-3.25	0
9	0	6	0	-3	0
9.25	0	6.25	1	-2.75	0
9.5	0	6.5	0	-2.5	0
9.75	0	6.75	1	-2.25	0

Availability Bin	Availability Frequency
10	0
10.25	0
10.5	0
10.75	1

Reliability Bin	Reliability Frequency
7	0
7.25	0
7.5	2
7.75	0
8	0
8.25	0
8.5	0
8.75	1
9	3

Security Bin	Security Frequency
-2	0
-1.75	0
-1.5	0
-1.25	0
-1	0
-0.75	0
-0.5	0
-0.25	0
0	32

Reliability Bin	Reliability Frequency	Security Bin	Security Frequency
9.25	0	0.25	0
9.5	0	0.5	0
9.75	1	0.75	0
10	0	1	0
10.25	0	1.25	0
10.5	0	1.5	0
10.75	4	1.75	0
11	0	2	0
11.25	0	2.25	0
11.5	0	2.5	0

Reliability Bin	Reliability Frequency
11.75	0
12	0
12.25	0
12.5	0
12.75	0
13	0
13.25	0
13.5	4
13.75	0
14	0

Security Bin	Security Frequency
2.75	0
3	0
3.25	0
3.5	0
3.75	0
4	0
4.25	0
4.5	6
4.75	4
5	10

Security Bin	Security Frequency
5.25	0
5.5	2
5.75	5
6	0
6.25	1
6.5	0
6.75	0
7	0
7.25	0
7.5	0

Security Bin	Security Frequency
7.75	0
8	0
8.25	0
8.5	0
8.75	0
9	0
9.25	1
9.5	0
9.75	6
10	2

Security Bin	Security Frequency
10.25	0
10.5	0
10.75	5
11	0
11.25	0
11.5	0
11.75	0
12	1
12.25	0

Security Bin	Security Frequency
12.5	0
12.75	0
13	0
13.25	0
13.5	0
13.75	0
14	0
14.25	0
14.5	3

Security Bin	Security Frequency
14.75	0
15	1
15.25	0
15.5	0
15.75	0
16	1
16.25	0
16.5	0
16.75	0
17	0

Security Bin	Security Frequency
17.25	0
17.5	0
17.75	1
18	0
18.25	0
18.5	0
18.75	1
19	0
19.25	0
19.5	0

Security Bin	Security Frequency
19.75	0
20	0
20.25	0
20.5	0
20.75	0
21	0
21.25	0
21.5	0
21.75	0
22	0

Security Bin	Security Frequency
22.25	0
22.5	0
22.75	0
23	0
23.25	0
23.5	0
23.75	0
24	0
24.25	0
24.5	0

Security Bin	Security Frequency
24.75	0
25	1
25.25	0
25.5	0
25.75	0
26	0
26.25	0
26.5	2

Histogram is created for each of the service parameters using these bin and frequencies. Histograms are created using Microsoft Excel. These histograms help to locate the 5% worst service values for each service parameter.

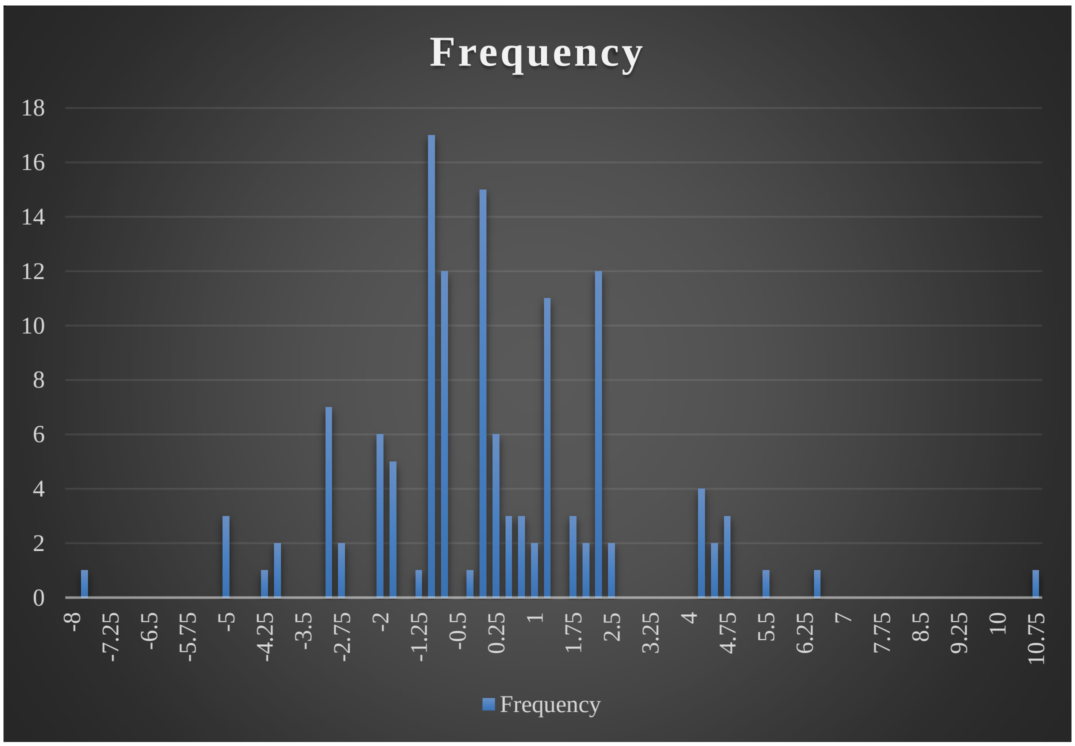

Figure 19: Availability Histogram

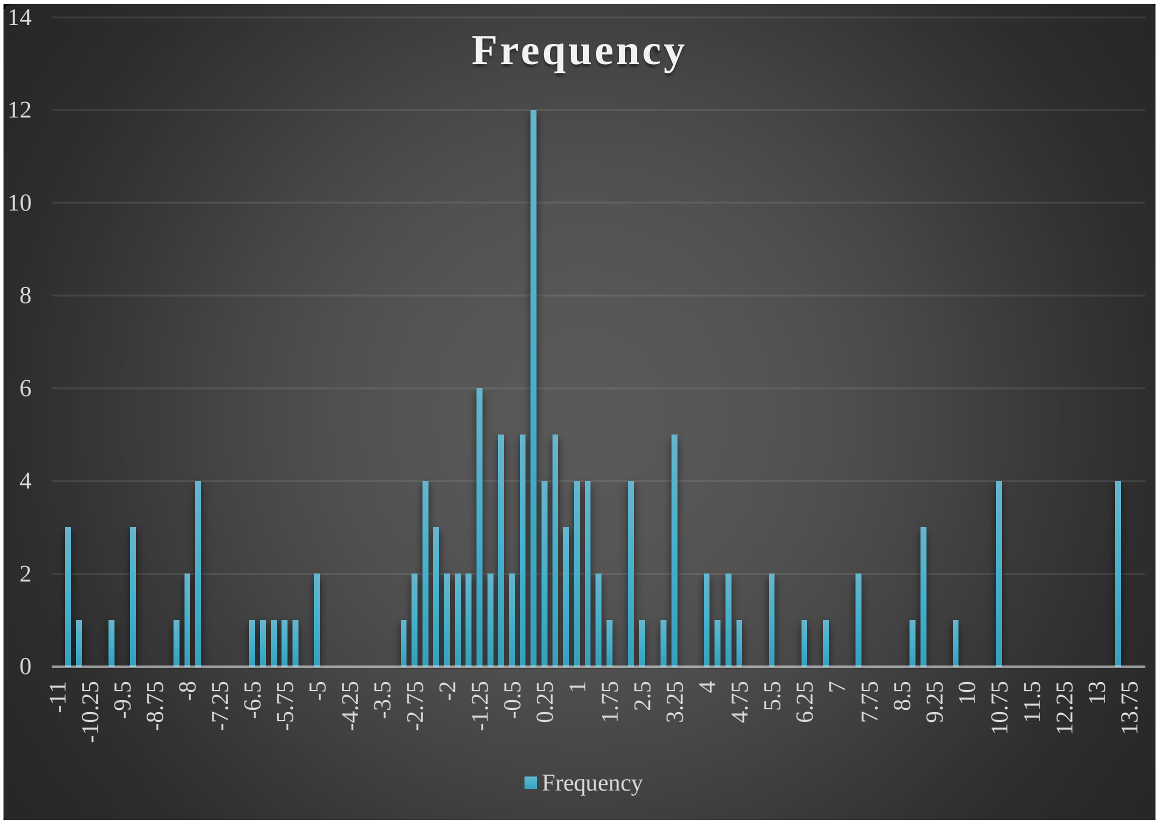

Figure 20: Reliability Histogram

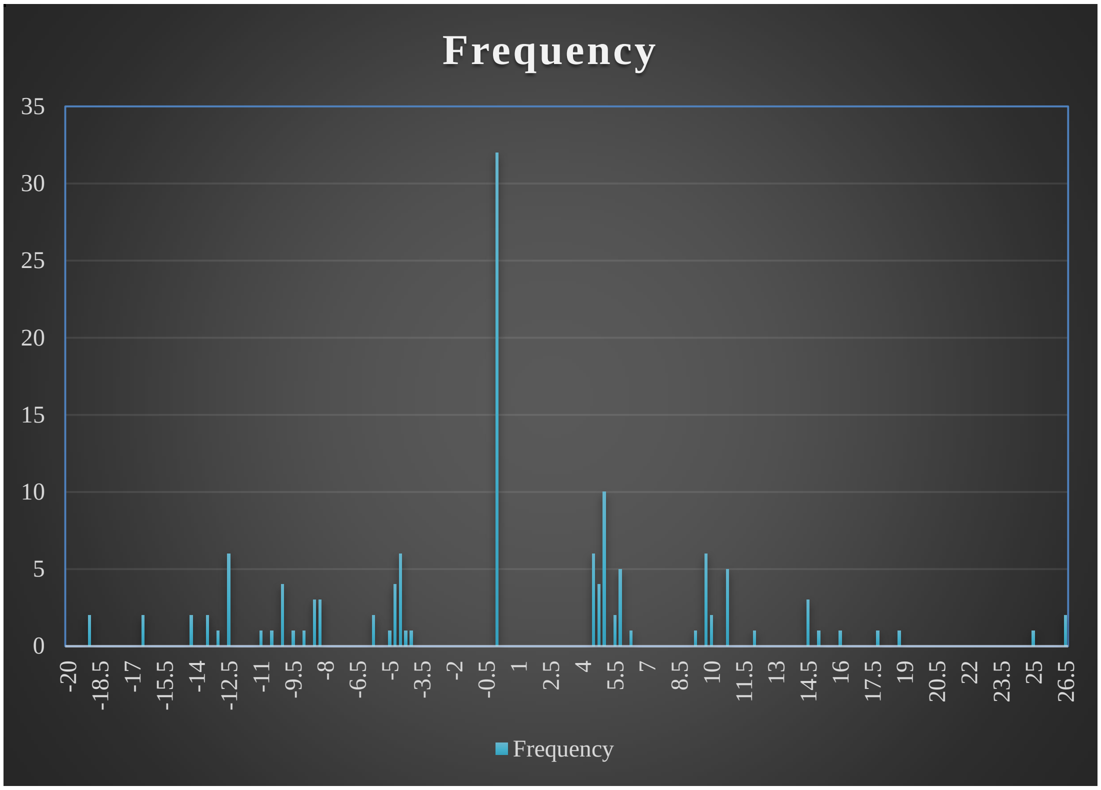

Figure 21: Security Histogram

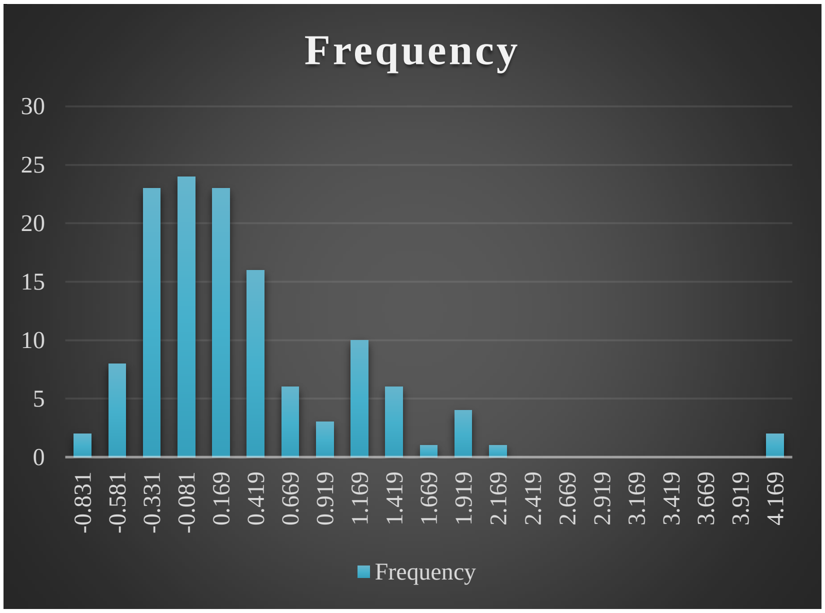

Figure 22: Response Time Histogram

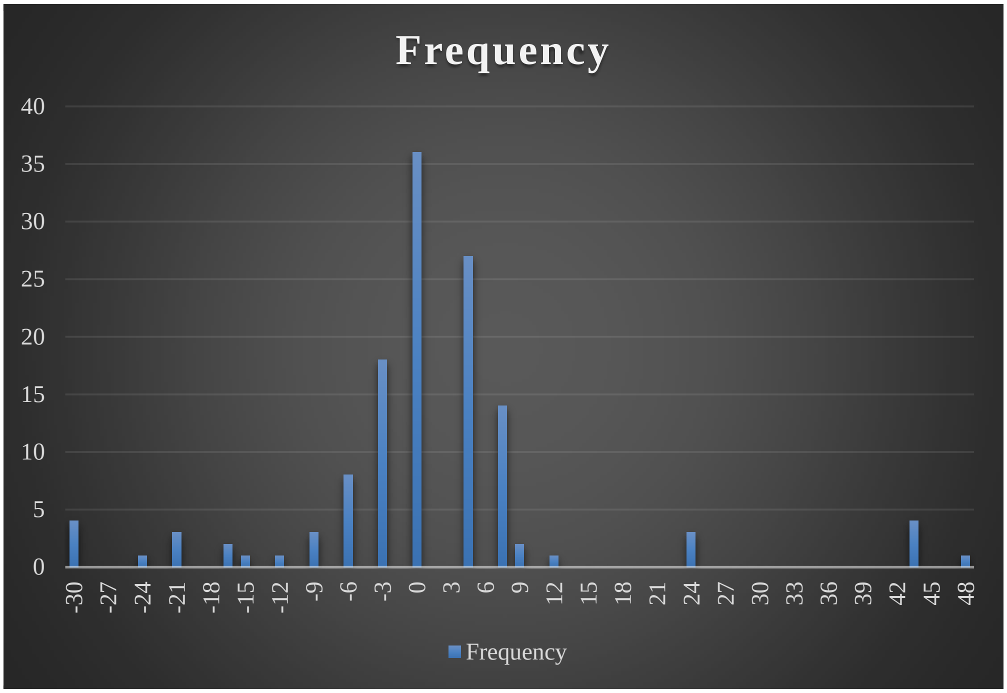

Figure 23: Data Storage Histogram

7.1. FINAL RESULTS

Table 29: Final Result Value at Risk

	Availability	Reliability	Security	Response Time	Data Storage
Highest fall of service level	-7.923	-10.885	-19.048	4.067	-30
Worst predicted value = Committed value-worst value	91.977	89.105	3.952	4.145	3070
Probability of such worst day to occur	0.007	0.007	0.007	0.007	0.007
Confidence level (Provider gives 95% confidence that worst day will not occur for consumer)	95.00%	95.00%	95.00%	95.00%	95.00%
Value at Risk with confidence level 95%	-4	-9.25	-14.25	1.919	-21
Final Predicted Value on worst day with 95% confidence level **Committed Value - Value at Risk**	95.90%	90.74%	7.75 hours	1.997 seconds	3079 GB

Let us understand all the steps involved to achieve the final results

Step 1: Requirement 2 has only one Eligible Cloud Provider C3

Step 2: Historic data is considered for past 6 months for this service

Step 3: I calculated the rise/fall values using the formula (x-(x-1))*100/(x-1) where x is the value for current day and x-1 is the service value for previous day.

Step 4: All the rise/fall values are shown in Appendix 1.

Step 5: Since we are interested to know the worst values, I consider fetching the highest fall in the service level for each parameter. This gives the worst possible values as shown in Table 27 and Table 29. It is possible that such worst service levels occur in a single day.

Step 6: I require knowing, how frequently the service levels fall to this level for past 6 months. This will help to predict the future of this service in terms of quality. This will give us the value for the unknown risk

Step 7: In order to get the frequency, I created bin and frequencies in the ascending order with worst fall values starting first.

Step 8: Using the bin and frequencies for each parameter in Table 28, histogram for created as shown in Figure 19-23

Step 9: The number of working days for which historic data is considered is 129 days, therefore probability of such worst service levels to occur in a single day is 1/129 which 0.007. This is shown in Equation 5

Equation 5: Calculating Probability

Probability (Worst Day) = 1/129 days = 0.007

Step 10: The probability of occurrence of such worst day is very less, in such situation let me assume the consumer considers that C3 is the only cloud provider which is meeting all the requirements so consumer may want to move ahead with this service.

Step 11: Both consumer and provider know the worst service levels can occur some day or in a month or a year. But, both of them wish to move ahead with the service, in such situation they both are taking risk. I need to calculate this value at risk. For this I introduce a term confidence level. Cloud provider gives a confidence level of 95% to the consumer that such worst service levels will not occur in a single day even though the probability of such occurrence is 0.007

Step 12: This clearly means that both provider and consumer are ready to take a risk of 5% because the confidence level by provider is only 95%.

Step 13: This means both consumer and provider are assuming that worst 5% of service values that occurred in past 6 months will not occur again.

Step 14: For this we fetch the worst 5% value at risk for each service parameter. Since total number of days is 129 so 5% of 129 = 6.45.

Step 15: This means worst 6-7 values occurred in the past for service parameters, will not occur again. We check the bin and frequencies Table 28 to calculate value at risk for each parameter. It is also shown in the histograms. It is included in the final result Table 29. This gave us value at risk for each parameter. Total risk of service can be calculated by sum of all the value at risk.

Step 16. As shown in final result table, we calculated the final predicted value by subtracting value at risk from the committed values given by the provider.

Step 17: Security is the most important priority for consumer with requirement 2 as shown in Table 18. The worst possible values in the final result Table 29 show that security can go very low this means that our model will give a high alert to the consumer to not move ahead with the cloud provider C3.

CHAPTER 8: CONCLUSION

We successfully evaluated Value at Risk for all the service level parameters, for requirement 2 and single cloud service provider C3 using our mentioned our formal model Similarly, we can evaluate risk for other requirements. Other requirements have more than one cloud provider, hence historic data will be analyzed for each provider and final result table will be prepared for each of these providers. After, achieving final results, comparison should be done about which provider gives the minimum risk and thus using our risk assessment model the consumer can make better decisions for the organization and the choose the best service along with minimum risk. Historic data plays a very important role in this model, therefore in order to make this model successful, it is important that the accurate historic data is provided by the provider of the cloud service. Such data can be monitored data or even the data collected during the testing the performance of the service in terms of availability, reliability and other parameters of a service. The service parameters can be changed or customized depending on a type of service. Our calculations and model will work for any type of parameters. It is simple and easy to implement even as a system. Each requirement stands as a requirement by a different consumer. So, if a single consumer has to use this model it will be very easy to do calculations even without actually developing a system. However, if more number of consumers and more service parameters are to include it is suggested to first develop a system based on this model and then use it. Additionally, we have assumed that this model is taking the inputs for a single type of service. It can be any type of service, but this entire model will work separately for each service as the parameter values will differ for different services.

REFERENCES

[1] Adams, R., & Bauer, E. (2012). Reliable Cloud Computing - Key Considerations. Cambridge: IEEE. Retrieved from http://www2.alcatel-lucent.com/techzine/wp-content/uploads/kalins-pdf/singles/reliable-cloud-computing-key-considerations.pdf

[2] Awodele, O., Ibikunle, F., & Kuyoro, S. O. (2011). Cloud Computing Security Issues and Challenges. *International Journal of Computer Networks, 3*(5).

[3] Bernsmed, K., Jaatun, M. G., & Undheim, A. (2012). Security SLAs – An Idea Whose Time Has Come? *7465*, 123-130. doi:10.1007/978-3-642-32498-7_10

[4] Bigelow, S. J. (2014, August). Five steps to moving mission-critical applications to the cloud. Retrieved from http://searchcloudcomputing.techtarget.com/tip/Five-steps-to-moving-mission-critical-applications-to-the-cloud

[5] Bills, D. (2014, January). *blogs.microsoft.com.* Retrieved from http://blogs.microsoft.com/cybertrust/2012/09/12/fundamentals-of-cloud-service-reliability/

[6] Biswas, S. (2011, February 8). Cloud Computing Risks (How to Deal with them?). Retrieved from http://cloudtweaks.com/2011/02/cloud-computing-risks-and-how-to-deal-with-them/

[7] Budnik, U. (2013, February). Lessons Learned from Recent Cloud Outages. Retrieved from http://www.rightscale.com/blog/enterprise-cloud-strategies/lessons-learned-recent-cloud-outages

[8] Chang, E., Chen, W., & Dillion, T. (2010). Cloud Computing : Issues and Challenges. *Advanced Information Networking and Applications (AINA)* (pp. 27-33). Perth: IEEE. doi:10.1109/AINA.2010.187

[9] Cloud Standard Overview. (2010). Retrieved from http://cloud-standards.org/wiki/index.php?title=Cloud_standards_overview

[10] Ercolani, G., & Murcia, U. d. (2013). Cloud Computing Services Potential Analysis. An integrated model for evaluating software as a service.

[11] Gartner. (n.d.). *The "SLA Way" to IT Success.* Retrieved from www.uptimesoftware.com: http://www.dabcc.com/documentlibrary/file/TheSLAWayToITSuccess.pdf

[12] Gulia, P., & Sood, S. (2013, June). Dynamic Ranking and Selection of Cloud Providers Using Service Level Agreements. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(6). Retrieved from http://www.ijarcsse.com/docs/papers/Volume_3/6_June2013/V3I6-0102.pdf

[13] Hefner, K. (2014, February). Cloud Outage. Retrieved from http://searchcloudstorage.techtarget.com/definition/cloud-outage

[14] Ko, R., & Lee, S. S. (2013, March). Cloud Computing Vulnerability incidents : A Statistical Overview.

[15] Mackay, M. (2013, December). Top Ten Outages in 2013.

[16] Mann, S. H., & Triantaphyllou, E. (1989, September). An examination of the effectiveness of multi-dimensional decision-making methods: a decision-making paradox. *Decision Support Systems, 5*(3), 303-312. doi:10.1016/0167-9236(89)90037-7

[17] McKendrick, J. (2013, August 17). Hidden Cost of Cloud Computing, Revealed. Retrieved from http://www.forbes.com/sites/joemckendrick/2013/07/17/hidden-costs-of-cloud-

[18] Miller, R. (2013, December 16). The year in Downtime: The top 10 Outages of 2013. Retrieved from http://www.datacenterknowledge.com/archives/2013/12/16/year-downtime-top-10-outages-2013/

[19] Myerson, J. M. (2013, January 07). Best practices to develop SLAs for cloud computing. Retrieved from http://www.ibm.com/developerworks/cloud/library/cl-slastandards/

[20] Peter Mell, T. G. (2011, September). *NIST (National Institue of Standards and Technology).* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[21] Raphael, J. (2011, June 27). The 10 worst cloud outages. Retrieved from http://www.infoworld.com/article/2622201/cloud-computing/the-10-worst-cloud-outages--and-what-we-can-learn-from-them-.html?page=2

[22] Rouse, M. (2014). Cloud Outage. Retrieved from http://searchcloudstorage.techtarget.com/definition/cloud-outage

[23] StellarPhoenixS. (2014, July 15). Cloud Computing is Increasingly becoming the rule and not the exception. Retrieved from http://wp.me/p2CITM-EA

[24] StellarPhoenixS. (2014, April 17). Top Myths Why Companies Avoid Adaption of Virtualization. Retrieved from http://wp.me/p2CITM-sR

[25] Vivek Nallur, R. B. (2009). Self Optimizing architechture for ensuring Quality Attributes in the cloud. (pp. 281-284). Cambridge: IEEE. Retrieved from https://www.cs.bham.ac.uk/~xin/papers/NullarBahsoonYaoWICSA09.pdf

APPENDIX 1 HISTORIC DATA FOR 6 MONTHS

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Thursday, January 10, 2013	99.920%		99.950%		22		8.300			3000	
Friday, January 11, 2013	99.000%	-0.921	99.090%	-0.860	21	-4.545	8.100	-2.410	-0.024	3000	0.000
Monday, January 14, 2013	99.095%	0.096	99.990%	0.908	22	4.762	7.700	-4.938	-0.049	3100	3.333
Tuesday, January 15, 2013	99.910%	0.822	99.000%	-0.990	21	-4.545	4.500	-41.558	-0.416	3100	0.000
Wednesday, January 16, 2013	98.000%	-1.912	94.000%	-5.051	23	9.524	4.700	4.444	0.044	3000	-3.226
Thursday, January 17, 2013	98.230%	0.235	96.000%	2.128	20	-13.043	9.900	110.638	1.106	2800	-6.667
Friday, January 18, 2013	99.000%	0.784	99.000%	3.125	20	0.000	9.300	-6.061	-0.061	3000	7.143
Monday, January 21, 2013	98.000%	-1.010	99.000%	0.000	23	15.000	4.500	-51.613	-0.516	3000	0.000

Thursday, January 31, 2013	Wednesday, January 30, 2013	Tuesday, January 29, 2013	Monday, January 28, 2013	Friday, January 25, 2013	Thursday, January 24, 2013	Wednesday, January 23, 2013	Tuesday, January 22, 2013	**Date**
99.910%	98.344%	99.098%	96.721%	99.500%	95.000%	97.000%	93.000%	**Availability**
1.592	-0.761	2.458	-2.793	4.737	-2.062	4.301	-5.102	**Rise/Fall Availability**
99.990%	99.000%	98.850%	98.850%	99.990%	98.500%	99.850%	99.983%	**Reliability**
1.000	0.152	0.000	-1.140	1.513	-1.352	-0.133	0.993	**Rise/Fall Reliability**
20	17	21	24	24	24	23	21	**Security**
17.647	-19.048	-12.500	0.000	0.000	4.348	9.524	-8.696	**Rise/Fall Security**
5.800	7.900	3.800	9.900	7.700	4.500	4.500	8.900	**Response Time *100**
-26.582	107.895	-61.616	28.571	71.111	0.000	-49.438	97.778	**Rise/Fall Response Time**
-0.266	1.079	-0.616	0.286	0.711	0.000	-0.494	0.978	**Actual Rise/fall Response**
3000	3000	3000	3000	3000	3000	3000	3000	**Data Storage**
0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	**Rise/Fall Data Storage**

Date	**Availability**	**Rise/Fall Availability**	**Reliability**	**Rise/Fall Reliability**	**Security**	**Rise/Fall Security**	**Response Time *100**	**Rise/Fall Response Time**	**Actual Rise/fall Response Time**	**Data Storage**	**Rise/Fall Data Storage**
Friday, February 01, 2013	99.090%	-0.821	94.000%	-5.991	21	5.000	9.800	68.966	0.690	3000	0.000
Monday, February 04, 2013	99.000%	-0.091	99.090%	5.415	22	4.762	4.800	-51.020	-0.510	3000	0.000
Tuesday, February 05, 2013	94.550%	-4.495	96.230%	-2.886	19	-13.636	3.900	-18.750	-0.188	3000	0.000
Wednesday, February 06, 2013	99.000%	4.707	96.880%	0.675	19	0.000	7.600	94.872	0.949	3000	0.000
Thursday, February 07, 2013	98.000%	-1.010	94.866%	-2.079	21	10.526	3.300	-56.579	-0.566	3000	0.000
Friday, February 08, 2013	97.000%	-1.020	98.889%	4.241	20	-4.762	7.800	136.364	1.364	3000	0.000
Monday, February 11, 2013	98.000%	1.031	98.889%	0.000	18	-10.000	6.800	-12.821	-0.128	3000	0.000
Tuesday, February 12, 2013	93.000%	-5.102	99.140%	0.254	19	5.556	9.900	45.588	0.456	3000	0.000

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response Time	Data Storage	Rise/Fall Data Storage
Wednesday, February 13, 2013	94.000%	1.075	93.560%	-5.628	19	0.000	7.900	-20.202	-0.202	3000	0.000
Thursday, February 14, 2013	99.000%	5.319	98.586%	5.372	19	0.000	5.600	-29.114	-0.291	3000	0.000
Friday, February 15, 2013	98.000%	-1.010	99.000%	0.420	22	15.789	8.800	57.143	0.571	2900	-3.333
Monday, February 18, 2013	93.000%	-5.102	97.589%	-1.425	23	4.545	7.700	-12.500	-0.125	3100	6.897
Tuesday, February 19, 2013	99.000%	6.452	91.258%	-6.487	24	4.348	8.700	12.987	0.130	2700	-12.903
Wednesday, February 20, 2013	98.000%	-1.010	93.856%	2.847	24	0.000	8.300	-4.598	-0.046	2900	7.407
Thursday, February 21, 2013	99.000%	1.020	99.986%	6.531	24	0.000	4.800	-42.169	-0.422	3000	3.448
Friday, February 22, 2013	99.990%	1.000	99.978%	-0.008	22	-8.333	9.700	102.083	1.021	3000	0.000

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Monday, February 25, 2013	99.900%	-0.090	98.256%	-1.722	24	9.091	9.400	-3.093	-0.031	3000	0.000
Tuesday, February 26, 2013	99.090%	-0.811	95.456%	-2.850	21	-12.500	4.500	-52.128	-0.521	3000	0.000
Wednesday, February 27, 2013	98.090%	-1.009	99.990%	4.750	23	9.524	2.500	-44.444	-0.444	3000	0.000
Thursday, February 28, 2013	96.080%	-2.049	97.850%	-2.140	21	-8.696	7.800	212.000	2.120	3000	0.000
Friday, March 01, 2013	99.980%	4.059	90.250%	-7.767	17	-19.048	7.100	-8.974	-0.090	3000	0.000
Monday, March 04, 2013	99.990%	0.010	89.860%	-0.432	17	0.000	7.900	11.268	0.113	3000	0.000
Tuesday, March 05, 2013	99.000%	-0.990	87.456%	-2.675	17	0.000	8.100	2.532	0.025	3000	0.000
Wednesday, March 06, 2013	97.980%	-1.030	99.258%	13.495	16	-5.882	8.800	8.642	0.086	3200	6.667

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Thursday, March 07, 2013	99.980%	2.041	88.579%	-10.759	20	25.000	4.500	-48.864	-0.489	2700	-15.625
Friday, March 08, 2013	99.890%	-0.090	87.879%	-0.790	19	-5.000	8.800	95.556	0.956	2900	7.407
Monday, March 11, 2013	97.990%	-1.902	91.285%	3.876	20	5.263	7.400	-15.909	-0.159	3100	6.897
Tuesday, March 12, 2013	95.980%	-2.051	89.568%	-1.881	21	5.000	4.800	-35.135	-0.351	3200	3.226
Wednesday, March 13, 2013	95.980%	0.000	98.980%	10.508	24	14.286	7.700	60.417	0.604	3000	-6.250
Thursday, March 14, 2013	99.990%	4.178	89.589%	-9.488	24	0.000	6.800	-11.688	-0.117	2100	-30.000
Friday, March 15, 2013	99.980%	-0.010	97.458%	8.783	21	-12.500	3.800	-44.118	-0.441	3000	42.857
Monday, March 18, 2013	98.880%	-1.100	98.457%	1.025	19	-9.524	7.800	105.263	1.053	3100	3.333

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Tuesday, March 19, 2013	97.480%	-1.416	99.145%	0.699	21	10.526	7.100	-8.974	-0.090	3100	0.000
Wednesday, March 20, 2013	98.990%	1.549	97.480%	-1.679	20	-4.762	8.900	25.352	0.254	3200	3.226
Thursday, March 21, 2013	99.000%	0.010	89.450%	-8.238	20	0.000	1.500	-83.146	-0.831	3100	-3.125
Friday, March 22, 2013	98.000%	-1.010	88.145%	-1.459	21	5.000	7.600	406.667	4.067	3200	3.226
Saturday, March 23, 2013	96.000%	-2.041	91.458%	3.759	18	-14.286	7.100	-6.579	-0.066	3100	-3.125
Sunday, March 24, 2013	97.980%	2.063	97.145%	6.218	18	0.000	7.000	-1.408	-0.014	3800	22.581
Monday, March 25, 2013	94.890%	-3.154	86.778%	-10.672	16	-11.111	6.400	-8.571	-0.086	3000	-21.053
Tuesday, March 26, 2013	96.880%	2.097	88.000%	1.408	17	6.250	3.900	-39.063	-0.391	2800	-6.667

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Wednesday, March 27, 2013	98.750%	1.930	89.000%	1.136	17	0.000	9.700	148.718	1.487	3100	10.714
Thursday, March 28, 2013	99.980%	1.246	97.485%	9.534	16	-5.882	9.100	-6.186	-0.062	3000	-3.226
Friday, March 29, 2013	99.090%	-0.890	98.890%	1.441	19	18.750	8.980	-1.319	-0.013	3000	0.000
Saturday, March 30, 2013	98.000%	-1.100	89.589%	-9.405	24	26.316	8.100	-9.800	-0.098	3100	3.333
Sunday, March 31, 2013	99.000%	1.020	97.458%	8.783	24	0.000	8.800	8.642	0.086	2900	-6.452
Monday, April 01, 2013	99.990%	1.000	97.480%	0.023	24	0.000	4.500	-48.864	-0.489	2800	-3.448
Tuesday, April 02, 2013	99.900%	-0.090	89.450%	-8.238	24	0.000	8.800	95.556	0.956	2900	3.571
Wednesday, April 03, 2013	99.090%	-0.811	98.980%	10.654	24	0.000	7.400	-15.909	-0.159	3000	3.448

Monday, April 15, 2013	Friday, April 12, 2013	Thursday, April 11, 2013	Wednesday, April 10, 2013	Tuesday, April 09, 2013	Monday, April 08, 2013	Friday, April 05, 2013	Thursday, April 04, 2013	**Date**
99.890%	99.980%	97.980%	99.000%	99.990%	99.980%	96.080%	98.090%	**Availability**
-0.090	2.041	-1.030	-0.990	0.010	4.059	-2.049	-1.009	**Rise/Fall Availability**
97.674%	98.115%	99.000%	96.875%	93.874%	99.874%	97.458%	89.589%	**Reliability**
-0.449	-0.894	2.194	3.197	-6.008	2.479	8.783	-9.488	**Rise/Fall Reliability**
21	20	20	24	24	24	24	24	**Security**
5.000	0.000	-16.667	0.000	0.000	0.000	0.000	0.000	**Rise/Fall Security**
1.500	8.900	7.100	7.800	3.800	6.800	7.700	4.800	**Response Time *100**
-83.146	25.352	-8.974	105.263	-44.118	-11.688	60.417	-35.135	**Rise/Fall Response Time**
-0.831	0.254	-0.090	1.053	-0.441	-0.117	0.604	-0.351	**Actual Rise/fall Response**
2600	2500	3000	3000	3100	2100	2800	3105	**Data Storage**
4.000	-16.667	0.000	-3.226	47.619	-25.000	-9.823	3.500	**Rise/Fall Data Storage**

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Tuesday, April 16, 2013	97.990%	-1.902	91.285%	-6.541	18	-14.286	7.600	406.667	4.067	2800	7.692
Wednesday, April 17, 2013	97.980%	-0.010	99.140%	8.605	19	5.556	7.100	-6.579	-0.066	2900	3.571
Thursday, April 18, 2013	94.890%	-3.154	99.990%	0.857	20	5.263	8.890	25.211	0.252	3100	6.897
Friday, April 19, 2013	96.880%	2.097	99.743%	-0.247	22	10.000	3.389	-61.879	-0.619	3000	-3.226
Monday, April 22, 2013	98.750%	1.930	97.897%	-1.851	21	-4.545	8.145	140.336	1.403	3100	3.333
Tuesday, April 23, 2013	97.980%	-0.780	89.578%	-8.498	21	0.000	4.560	-44.015	-0.440	3000	-3.226
Wednesday, April 24, 2013	99.980%	2.041	99.012%	10.532	23	9.524	3.450	-24.342	-0.243	3200	6.667
Thursday, April 25, 2013	99.890%	-0.090	88.235%	-10.885	24	4.348	9.415	172.899	1.729	3000	-6.250

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Friday, April 26, 2013	97.990%	-1.902	94.789%	7.428	22	-8.333	3.339	-64.535	-0.645	2100	-30.000
Monday, April 29, 2013	97.980%	-0.010	98.889%	4.325	21	-4.545	4.561	36.598	0.366	3000	42.857
Tuesday, April 30, 2013	94.890%	-3.154	98.889%	0.000	20	-4.762	5.891	29.160	0.292	3100	3.333
Wednesday, May 01, 2013	99.000%	4.331	99.140%	0.254	18	-10.000	3.457	-41.317	-0.413	3100	0.000
Thursday, May 02, 2013	99.990%	1.000	97.850%	-1.301	19	5.556	3.458	0.029	0.000	3200	3.226
Friday, May 03, 2013	99.900%	-0.090	90.250%	-7.767	21	10.526	3.330	-3.702	-0.037	3100	-3.125
Saturday, May 04, 2013	99.090%	-0.811	89.860%	-0.432	22	4.762	6.456	93.874	0.939	3200	3.226
Sunday, May 05, 2013	98.090%	-1.009	87.456%	-2.675	19	-13.636	5.810	-10.006	-0.100	3100	-3.125

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Monday, May 06, 2013	96.080%	-2.049	99.258%	13.495	24	26.316	9.481	63.184	0.632	3800	22.581
Tuesday, May 07, 2013	99.980%	4.059	96.875%	-2.401	21	-12.500	7.880	-16.886	-0.169	3000	-21.053
Wednesday, May 08, 2013	99.990%	0.010	96.789%	-0.089	24	14.286	6.661	-15.470	-0.155	3100	3.333
Thursday, May 09, 2013	99.000%	-0.990	99.785%	3.095	23	-4.167	3.214	-51.749	-0.517	3000	-3.226
Friday, May 10, 2013	95.000%	-4.040	99.900%	0.115	22	-4.348	7.100	120.909	1.209	3000	0.000
Monday, May 13, 2013	99.500%	4.737	99.258%	-0.643	22	0.000	8.890	25.211	0.252	2500	-16.667
Tuesday, May 14, 2013	96.721%	-2.793	99.999%	0.747	23	4.545	3.389	-61.879	-0.619	2600	4.000
Wednesday, May 15, 2013	99.098%	2.458	99.097%	-0.902	24	4.348	8.145	140.336	1.403	2800	7.692

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Thursday, May 16, 2013	98.344%	-0.761	99.012%	-0.086	20	-16.667	4.560	-44.015	-0.440	2900	3.571
Friday, May 17, 2013	99.910%	1.592	97.850%	-1.174	18	-10.000	3.450	-24.342	-0.243	3100	6.897
Monday, May 20, 2013	97.980%	-1.932	90.250%	-7.767	19	5.556	9.415	172.899	1.729	2800	-9.677
Tuesday, May 21, 2013	94.890%	-3.154	89.860%	-0.432	17	-10.526	3.339	-64.535	-0.645	2900	3.571
Wednesday, May 22, 2013	96.880%	2.097	87.456%	-2.675	19	11.765	4.561	36.598	0.366	3100	6.897
Thursday, May 23, 2013	97.980%	1.135	99.258%	13.495	21	10.526	5.891	29.160	0.292	3000	-3.226
Friday, May 24, 2013	94.890%	-3.154	96.875%	-2.401	22	4.762	3.457	-41.317	-0.413	3100	3.333
Monday, May 27, 2013	96.880%	2.097	99.000%	2.194	23	4.545	9.648	179.086	1.791	3000	-3.226

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Tuesday, May 28, 2013	97.578%	0.720	94.000%	-5.051	23	0.000	9.568	-0.829	-0.008	3200	6.667
Wednesday, May 29, 2013	97.980%	0.412	96.000%	2.128	24	4.348	8.890	-7.086	-0.071	3000	-6.250
Thursday, May 30, 2013	90.217%	-7.923	99.000%	3.125	24	0.000	6.458	-27.357	-0.274	2100	-30.000
Friday, May 31, 2013	89.987%	-0.255	99.000%	0.000	21	-12.500	7.589	17.513	0.175	3000	42.857
Monday, June 03, 2013	99.580%	10.660	99.983%	0.993	22	4.762	4.562	-39.887	-0.399	2700	-10.000
Tuesday, June 04, 2013	99.990%	0.412	99.850%	-0.133	21	-4.545	3.485	-23.608	-0.236	2900	7.407
Wednesday, June 05, 2013	99.990%	0.000	98.500%	-1.352	21	0.000	3.257	-6.542	-0.065	3100	6.897
Thursday, June 06, 2013	99.990%	0.000	98.871%	0.377	21	0.000	4.257	30.703	0.307	3200	3.226

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Friday, June 07, 2013	98.981%	-1.009	99.999%	1.141	24	14.286	4.125	-3.101	-0.031	3000	-6.250
Saturday, June 08, 2013	97.980%	-1.011	96.789%	-3.210	22	-8.333	3.214	-22.085	-0.221	2100	-30.000
Sunday, June 09, 2013	94.890%	-3.154	99.785%	3.095	20	-9.091	7.100	120.909	1.209	3000	42.857
Monday, June 10, 2013	96.880%	2.097	99.900%	0.115	18	-10.000	8.890	25.211	0.252	3100	3.333
Tuesday, June 11, 2013	97.980%	1.135	99.258%	-0.643	19	5.556	3.389	-61.879	-0.619	3100	0.000
Wednesday, June 12, 2013	94.890%	-3.154	89.578%	-9.752	21	10.526	8.145	140.336	1.403	3200	3.226
Thursday, June 13, 2013	96.880%	2.097	99.012%	10.532	22	4.762	4.560	-44.015	-0.440	3100	-3.125
Friday, June 14, 2013	97.578%	0.720	88.235%	-10.885	23	4.545	3.450	-24.342	-0.243	3200	3.226

Date	Availability	Rise/Fall Availability	Reliability	Rise/Fall Reliability	Security	Rise/Fall Security	Response Time *100	Rise/Fall Response Time	Actual Rise/fall Response	Data Storage	Rise/Fall Data Storage
Monday, June 17, 2013	97.980%	0.412	94.789%	7.428	24	4.348	9.415	172.899	1.729	3100	-3.125
Tuesday, June 18, 2013	99.990%	2.051	98.889%	4.325	24	0.000	3.339	-64.535	-0.645	3800	22.581
Wednesday, June 19, 2013	99.990%	0.000	98.889%	0.000	24	0.000	4.561	36.598	0.366	3000	-21.053
Thursday, June 20, 2013	98.981%	-1.009	99.140%	0.254	21	-12.500	5.891	29.160	0.292	2800	-6.667
Friday, June 21, 2013	99.990%	1.019	97.850%	-1.301	20	-4.762	3.457	-41.317	-0.413	2900	3.571
Monday, June 24, 2013	99.990%	0.000	90.250%	-7.767	22	10.000	6.485	87.590	0.876	3100	6.897
Tuesday, June 25, 2013	98.981%	-1.009	89.860%	-0.432	21	-4.545	2.561	-60.509	-0.605	3000	-3.226
Wednesday, June 26, 2013	94.890%	-4.133	87.456%	-2.675	23	9.524	3.245	26.708	0.267	3100	3.333

Friday, June 28, 2013	Thursday, June 27, 2013	**Date**
97.578%	96.880%	**Availability**
0.720	2.097	**Rise/Fall Availability**
96.875%	99.258%	**Reliability**
-2.401	13.495	**Rise/Fall Reliability**
23	21	**Security**
9.524	-8.696	**Rise/Fall Security**
6.458	4.897	**Response Time *100**
31.877	50.909	**Rise/Fall Response Time**
0.319	0.509	**Actual Rise/fall Response**
3000	3000	**Data Storage**
0.000	-3.226	**Rise/Fall Data Storage**

APPENDIX 2 IRB APPROVAL LETTER

EAST CAROLINA UNIVERSITY
University & Medical Center Institutional Review Board Office
4N-70 Brody Medical Sciences Building· Mail Stop 682
600 Moye Boulevard · Greenville, NC 27834

Office **252-744-2914** · Fax **252-744-2284** · **www.ecu.edu/irb**

Notification of Exempt Certification

From: Social/Behavioral IRB
To: Komal Hotwani
CC:
Nasseh Tabrizi
Nasseh Tabrizi
Date: 9/24/2014
Re: UMCIRB 14-001405
Formal Model to reduce the risk of cloud outages.

I am pleased to inform you that your research submission has been certified as exempt on 9/24/2014 . This study is eligible for Exempt Certification under category #2 .

It is your responsibility to ensure that this research is conducted in the manner reported in your application and/or protocol, as well as being consistent with the ethical principles of the Belmont Report and your profession.

This research study does not require any additional interaction with the UMCIRB unless there are proposed changes to this study. Any change, prior to implementing that change, must be submitted to the UMCIRB for review and approval. The UMCIRB will determine if the change impacts the eligibility of the research for exempt status. If more substantive review is required, you will be notified within five business days.

The UMCIRB office will hold your exemption application for a period of five years from the date of this letter. If you wish to continue this protocol beyond this period, you will need to submit an Exemption Certification request at least 30 days before the end of the five year period.

The Chairperson (or designee) does not have a potential for conflict of interest on this study.

IRB00000705 East Carolina U IRB #1 (Biomedical) IORG0000418
IRB00003781 East Carolina U IRB #2 (Behavioral/SS) IORG0000418