2014

Cloud Computing: Challenges And Risk Management Framework

Madallah Almadallah
North Carolina Agricultural and Technical State University

Cloud Computing: Challenges and Risk Management Framework

Madallah Almadallah

North Carolina A&T State University

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Department: Computer and Information Technology

Major: Information Technology

Major Professor: Dr. Ibraheem Kateeb

Greensboro, North Carolina

2014

The Graduate School
North Carolina Agricultural and Technical State University
This is to certify that the Master's Thesis of

Madallah Almadallah

Has met the thesis requirements of
North Carolina Agricultural and Technical State University

Greensboro, North Carolina
2014

Approved by:

Dr. Ibraheem Kateeb Major Professor	Dr. Evelyn Sowells Committee Member
Dr. Rajeev Agrawal Committee Member	Dr. Naser El-Bathy Committee Member

Dr. Clay S. Gloster
Department Chair

Dr. Sanjiv Sarin
Dean, The Graduate School

Biographical Sketch

Mr. Madallah Almadallah is currently a graduate student in Department of Electronics, Computer and Information Technology School of Technology at North Carolina Agricultural and Technical State University in Greensboro. He graduated from Elon University in Elon with a bachelor degree in Computer Information System in 2013.

His research interest areas include cloud computing, security and IT management. He has published and presented two researches: one at IEEE SoutheastCon 2014 (entitled "The Future of Cloud Computing: Security and Network Threats of IT Industry") and one at the 4th IAJC/ISAM Joint International Conference (entitled "Cloud Computing in Business: Risk Management Framework").

Dedication

I would like to dedicate my thesis to my beloved parents, wife and children.

Acknowledgements

I would like to thank my committee chair and advisor professor Dr. Ibraheem Kateeb who has been a constant source of knowledge and inspiration. He was always available for my questions and he was positive and gave generously of his time and knowledge.

In addition, my sincere thanks to my Professor Dr. Evelyn Sowells for her encouragements, insightful comments, immense knowledge and the willing to always help all throughout my graduate research.

Finally, special thanks to the department chair Dr. Clay S. Gloster and the committee members Dr. Naser El-Bathy and Dr. Rajeev Agrawal for their time and support. Their contribution and inputs helped me in my research and writing of this thesis.

Table of Contents

List of Figures

List of Tables

Abstract

Cloud-computing technology has developed rapidly. It can be found in a wide range of social, business and computing applications. Cloud computing would change the Internet into a new computing and collaborative platform. It is a business model that achieves purchase on-demand and pay-per-use in network. Many competitors, organizations and companies in the industry have jumped into cloud computing and implemented it.

Cloud computing provides us with things such as convenience, reduced cost and high scalability. But despite all of these advantages, there are many enterprises, individual users and organizations that still have not deployed this innovative technology. Several reasons lead to this problem; however, the main concerns are related to security, privacy and trust. Low trust between users and cloud computing providers has been found in the literature.

It is important to note that choosing cloud computing assumes a high degree of trust between the organization and its cloud computing provider, as the provider will be trusted with sensitive information and security details. In an attempt to solve the problem and increase the investment and adoption of this technology, this thesis provides a comprehensive cloud computing risk management framework based on previous work.

This Risk Management Framework consists of six stages, namely: (1) understand the business context, (2) identify the business technical risk, (3) synthesize and prioritize the risk, (4) define the risk mitigation strategy, (5) carry out required solutions and validate that they are resolved and (6) overall assessment and monitoring of the system. The first five steps are the well-known risk management stages, but this research has adopted a more robust approach to each of them. The sixth stage is a new stage that is unique to this work. This thesis highlights the details of these approaches used in the first five steps as well as the explanation of the sixth step.

A scenario explaining a step-by-step approach to applying this Risk Management Framework to a hypothetical cloud computing provider has been outlined. The advantage of this Risk Management Framework lies in the fact that it can be used in wide range and flexibility because it can fit with small and large enterprise. Also, it is not specific to security risks; it can be applied in non-software situations.

CHAPTER 1

Introduction

Over the past few years, Internet has been developing very rapidly in wide range. It has become available and accessible for everyone. However, other issues such as storage size, the power consumed by equipment and hardware cost have been constantly increasing. The storage space in data center is no longer meeting our increasing demands. The innovation of cloud computing has emerged in an attempt to solve these and other environmental problems. This has changed the phase of Information Technology (IT) industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased.

Cloud computing has become popular in the IT industry. It is a virtual server available over the Internet; that enables the user to access computing resources and services, regardless of time and place. Well-known cloud computing providers include Amazon Web Services (AWS), Microsoft Windows Azure, and Google AppEngine.

In the 1960s, John McCarthy introduced the fundamental concept of cloud computing (Jadeja & Modi, 2012). He believed that "computation may some day be organized as a public utility" (Jadeja & Modi, 2012, p. 877). The term cloud came from the telecommunications world, where telecom companies started offering high quality Virtual Private Network (VPN) services at a much lower cost (Jadeja & Modi, 2012). By using VPN services, these companies can switch traffic to balance utilization of the overall network. Now, Cloud computing extends this to cover servers and network infrastructure.

The origin of the term “cloud computing” is unclear. Bento and Bento (2011) stated “The term only gained traction around 2006 or 2007, but we found references dating back from much earlier. For example, a 1997 MIT paper (Gillett & Kapor) showed a figure about the

Internet's confederation approach, with the drawing of a cloud (labeled "cloud" of intermediate networks), to which originating and receiving networks were connected through routers." (p. 41). Formally, CEO Eric Schmidt used the term "cloud computing" at a search engine conference in 2006 to describe what they were doing in terms of Software as Service (SaaS). Weeks later, Amazon used the word "cloud" when it launched its EC2 "elastic computing cloud" services, and the term entered the mainstream (Bento & Bento, 2011).

Despite all the advantages of using cloud computing, there are some associated threats and risks. These issues can reduce the confidence of using this new innovation, especially among individual users and small enterprises, organizations and businesses. This thesis seeks to bring greater clarity landscape about cloud computing threats that are mainly related to security. Also, it emphasizes the use of Risk Management Framework plan to deal with security issues within cloud computing.

1.1 Overview of Cloud Computing

1.1.1 Definition

In fact, there is no agreement on the cloud computing definition; different people subscribe to different definitions of cloud computing. Thus, multiple definitions are found, varying from very broad to very narrow and emphasizing the perspective of different stakeholders. Despite this fact, the primary goal of cloud computing is to provide on-demand computing services with high reliability, scalability, and availability in distributed environments. The main objective of cloud computing is to make better use of distributed resources and solve large-scale computation problems (Sadiku, Musa & Momoh, 2014).

The US National Institute of Standards and Technology (NIST) provided a standard definition as: "a model for enabling convenient, on-demand network access to a shared pool of

configuration computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Han, 2011, p. 199; Bento & Bento, 2011, p.42; Mell & Grance, 2011; Xu, 2012, p. 75). Cisco Systems defines cloud computing as "IT resources and services that are abstracted from the underlying infrastructure and provided 'on-demand' and 'at scale' in a multitenant environment" (Rimal, Jukan, Katsaros & Goeleven, 2010, p. 3). Also, cloud computing is defined as "a pay-per-use model for enabling available, convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Wang, 2011, p. 436). Vaquero et al, (2009, cited in Qaisar & Khawaja, 2012) defines cloud computing as

> Clouds are a large pool of easily and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the infrastructure provider by means of customized service-level Agreements (p. 1324).

Different definitions focusing on the technical aspects of the cloud computing has been rendered such as: "Cloud computing is grid computing, the use of a distributed network of servers, each working in parallel, to accomplish a specific task. As an acquaintance of mine put it, if it isn't using MapReduce, it probably isn't a cloud" (Bento & Bento, 2011, p. 41). A comprehensive review conducted in 2009 by the University of California Berkeley RAD Lab (Reliable Adaptive Distributed Systems Laboratory) yielded a definition that has been gaining broad popularity: "Cloud Computing refers to both the applications delivered as services over the

Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud" (Wang, Wang, & Huang, 2011, p. 404; Armbrust, et.al, 2010, p. 51; Bento & Bento, 2011, p.41).

However, there are common characteristics and features that can be found. According to NIST, the cloud computing model consists of five essential characteristics, three service models and four deployment models (Mell & Grance, 2011). The characteristics are described as on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service (Mell & Grance, 2011). Wang, Wang and Huang (2011) introduced six characters of cloud computing: ultra large-scale; virtualization; high reliability; versatility; high extendibility; on demand service; and extremely inexpensive. While Jadeja and Modi (2012), identified the characteristics of cloud computing as the following:

- Users can access the data, applications or any other services with the help of a browser regardless of the device used and the user's location. The infrastructure, which is generally provided by a third-party, is accessed with the help of Internet.
- Less Information Technology (IT) skills are required for implementation.
- Reliable service can be obtained by the use of multiple sites.
- Sharing of resources and costs amongst a large number of users allows efficient utilization of the infrastructure.
- Maintenance is easier in case of cloud computing applications, as they need not be installed on each user's computer.
- Pay per use facility allows measuring the usage of application per client on regular bases.
- Performance can be monitored and thus it is scalable.

- Security can be as good as or better than traditional systems because providers are able to devote resources to solving security issues that many customers cannot afford. However, security still remains an important concern when the data is quite confidential. This delays adoption of cloud computing to some extent (p. 877-878).

Cloud computing also has a lot of characteristics including Shared Infrastructure, Handle Metering and Network Access. Shared Infrastructure is one Cloud computing uses a software/application model that allows sharing of physical services, storage and network capabilities among users. Handle Metering can be easily described as keeping records of usage of service by clients. This is used by the cloud computing providers for optimization and to bill the clients according to their cloud resource usage, as you are only going to be billed when you use and on the amount of usage. Network Access is were Cloud computing is accessed over a network by a wide range of devices like PCs, laptops, mobile devices by using standard APIs.

1.1.2 Service models

In literature and practice, there are three common types of service delivery cloud computing models namely: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) (Wang, 2011; Mell& Grance, 2011). Conceptually, in Cloud Computing everything is assumed as a service (XaaS) (Rimal, et, al., 2010; Xu, 2012). These services define the layered system structure for cloud computing see Figure 1. Xu (2012) said

> At the Infrastructure layer, processing, storage, networks, and other fundamental computing resources are defined as standardized services over the network. The middle layer, i.e. PaaS, provides abstractions and services for developing, testing, deploying, hosting, and maintaining applications in the integrated development environment. The application layer provides a complete application set of SaaS.

The user interface layer at the top enables seamless interaction with all the underlying XaaS layers.

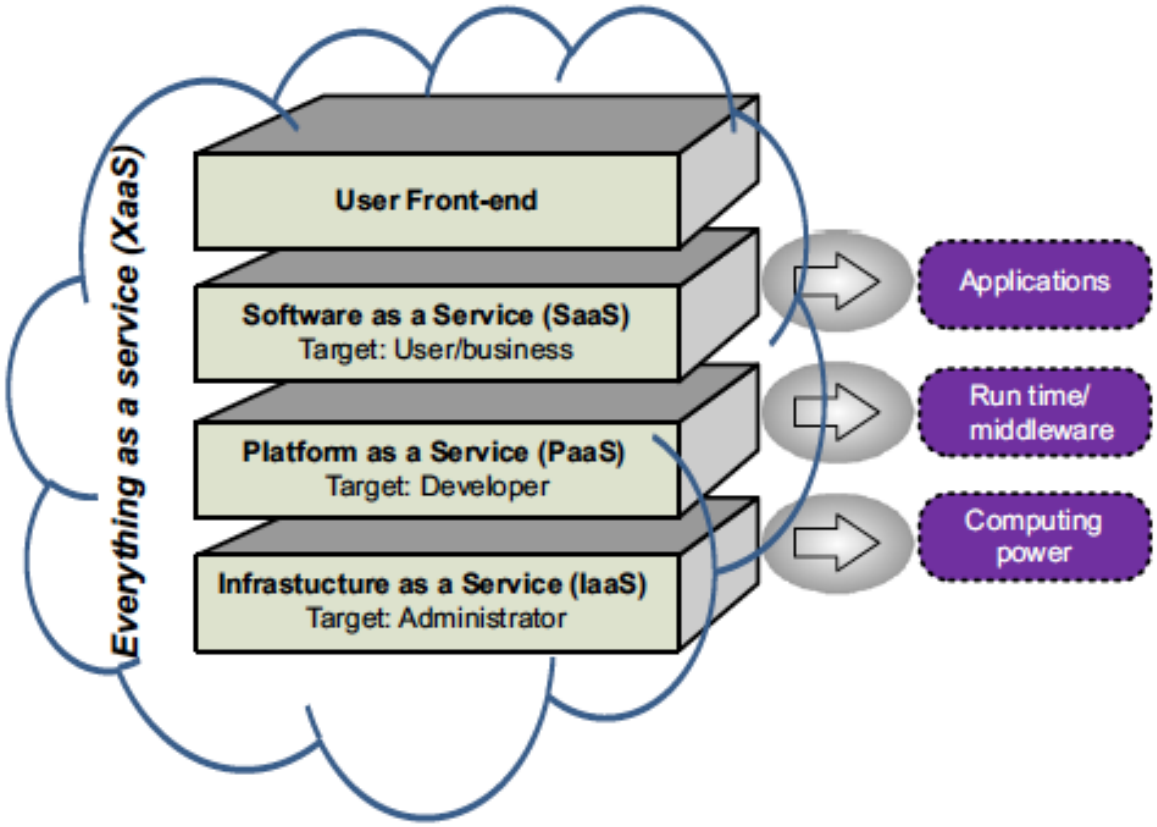

Figure 1: Cloud computing: everything is a service.

SaaS is sometimes referred to as Application as a Service (AaaS) and Application Service Provider (ASP) model (Xu, 2012). Mell and Grance (2011) explained SaaS as, "The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure.

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface" (p. 2). SaaS is the application that a cloud service provider runs to enables its users to use these applications through network, basically the Internet see Figure 2. According to Han (2011), the cloud

computing providers manage almost everything in the cloud infrastructure, such as physical servers, network, OS and applications, in the SaaS model. This model is designed specifically for general end users. The end users are able to run applications on the clouds and they are not required to install, upgrade, and backup applications and their work. Examples of the key providers are the Sales force Customer Relationships Management (CRM) system, NetSuite, and Google Office Productivity application. Some examples of SaaS products are Google Apps and Salesforce Sales CRM (Han, 2011).

PaaS model is a development tool that supports and helps users to build Web applications without installing any tools. General software developers are target group in this model. It provides developers with a platform allowing them to develop, test, deploy and host sophisticated web applications as a service delivered by a cloud-based platform (Xu, 2012). "Compared with conventional application development, PaaS can significantly reduce the development time, and also offers hundreds of readily available services. PaaS provides a solution for offering multiple applications on the same platform thus increasing the economy of scale and reducing complexity" (Rimal, et, al., 2010, p. 8). In addition, using this service does not require any special knowledge, skills or expertise (Qaisar & Khawaja, 2012). In this model, the cloud computing providers manage everything except the application in the cloud infrastructure (Han, 2011). Google AppEngine, Windows Azure, Facebook F8, Salesforge App Exchange, Bunzee connect and Amazon EC2 and Joyent are considered to be examples of PaaS model see Figure 2 and Table 1).

IaaS is sometimes called Hardware as a Service (HaaS) (Xu, 2012) see Figure 2. The cloud service providers only operate, maintain and control physical cloud infrastructure in this model such as storage, hardware, server and networking (Qaisar &

Khawaja, 2012). However, this model allows users to manage processing, storage, networks, and other fundamental computing resources; they can use and run arbitrary software such as operating systems and applications (Han, 2011). As a result, the users have maximum control on the infrastructure as if they own underlying physical servers and network. There are two extremely useful advantages of using this model for enterprise users: it reduces the need for investing in building and managing IT systems; another important benefit is the ability of having access to the latest technology as it emerges (Xu, 2012). According to Rimal et, al., (2010), on-demand, self-sustaining or self-healing, multi-tenant, customer segregation are the key requirements of IaaS. Leading providers of this model includes Amazon, Linode, Rackspace, Joyent, and IBM Blue Cloud (Han, 2011). Some examples of IaaS include GoGrid, Mosso/Rackspace, MSP On- Demand, and masterIT.

Figure 2: Cloud computing service models.

1.1.3 Deployment models

In ordered to understand the complexity of cloud computing and its relationship with business and other fields, fundamental information of cloud computing deployment models

should be highlighted. In terms of deployment, NIST distinguishes between private clouds, public clouds, community clouds and hybrid clouds (Mell& Grance, 2011) see Figure 3.

Table 1

List of Major Cloud Computing providers

Cloud Computing Provider	Layer
Akamai	PaaS, SaaS
Amazon Web Services	IaaS, PaaS, SaaS
EMC	SaaS
Eucalyptus	IaaS open source software
Google	PaaS(AppEngine), SaaS
IBM	Paas, SaaS
Linode	IaaS
Microsoft	PaaS, (Azure), Saas
Rackspace	IaaS, PaaS, SaaS
Salesforce.com	PaaS, SaaS
VMware vCloud	PaaS, IaaS
Zoho	SaaS

Public cloud is designed for general public over the Internet on a pay-as-you-go basis and provided by a third party vendor. It provides resources, web applications and web services for any user (Qaisar & Khawaja, 2012). However, consumers have little control over the infrastructure (Brohi & Bamiah, 2011). For example, the Amazon Elastic Compute Cloud (EC2)

allows users to rent virtual machine to run their own applications. Eucalyptus is an open-source cloud computing system developed by the University of California at Santa Barbara (Han, 2011).

Private cloud is designed for a single organization comprising multiple consumers (e.g., business units). The data services and web applications within the organization cloud are only used by the organization's members. However, the cloud may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises (Mell& Grance, 2011). For example, Microsoft Azure enables customers to build their own private clouds. The main advantage in using private cloud is that it is easier to manage security, maintenance and also provides more control over the deployment and use (Jadeja & Modi, 2012). Although private clouds offer several similar benefits to those of public clouds, the enterprise using private cloud is in charge of setting up and maintaining the cloud, which is the major difference between these two types. Brohi and Bamiah (2011) stated, "The difficulty and cost of establishing an internal cloud can be very expensive, and the cost of continual operation of the cloud might exceed the cost of using a public cloud. Private clouds offer some advantages compared to public clouds such as control over managing the cloud. Organizations feel in control over their cloud services and security".

Community clouds consist of one or more public, private or hybrid clouds. The purpose of this cloud is to serve common concerns such as security, policy or mission by collaboration of several organizations (Qaisar & Khawaja, 2012). For example, Google provides GovCloud for Los Angeles City Council; city's formal agencies are the only users who can access to this data. "The cloud infrastructure can be hosted by a third-party vendor or one of the organizations within the community" (Brohi & Bamiah, 2011, p. 288).

Hybrid clouds consist of one or more public, private or community clouds. These clouds would typically be created by the enterprise, and management responsibilities would be split between the enterprise and the cloud provider (Brohi & Bamiah, 2011). The organization can also maintain and manage its own data and other organizations data. For example, "overflow cloud" is created by IBM and Juniper Networks across IBM's worldwide Cloud Labs for customer engagements (Qaisar & Khawaja, 2012). According to Brohi and Bamiah (2011), the major challenge with this type is the difficulty in effectively creating and governing such a solution. Also, another challenge is that services from different sources must be obtained and provisioned as if they originated from a single location. Finally, the relations between private and public clouds can make the implementation even more complicated.

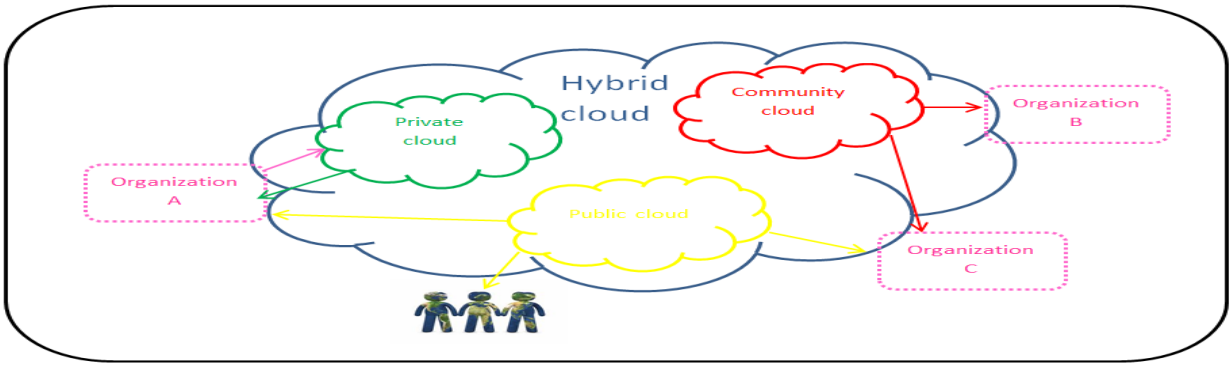

Figure 3: Cloud computing deployment models.

It is important to understand the fundamental structure of cloud computing. This chapter has given an overview of cloud computing including definition, common characteristics, architecture and models. Cloud computing has powerful features, basically in business environment. The next chapter, literature review, will address the advantages, risks and problems of cloud computing. However, the focus will be on the threats and their negative impacts on clients' (e.g. adaptors and users) trust and usages.

CHAPTER 2

Literature Review

2.1 Research Problems

This thesis highlights the overview, benefits and security challenges of cloud computing. The main problem discussed in this thesis is that, several security risks and problems occur when using cloud computing on both sides: users and providers. These problems can decrease the level of trust between the users and providers. Also, as more security incidents occur, more people develop worries about using the cloud. On the one side, providers need to be able to detect and deal with security risks and problems before, during and after they occur. Thus, a risk management framework for dealing with few security issues was proposed from the cloud providers' perspective. The two main goals were to increase confidence between the users and cloud provider and to increase the use of cloud computing in all levels.

2.2 Literature Review

In the last seven years, the field of cloud computing has been significantly developed. There are a growing number of articles related to cloud computing in libraries. Cloud computing is the advanced picture of various technologies such as grid computing, distributed computing and Service-oriented Architecture (SOA) (Brohi & Bamiah, 2011). Cloud computing involves three types of stakeholders, which are providers (i.e. IT industries), adopters (i.e. business and organizations) and users see Figure 4. However, Marston, Li, Bandyopadhyay, Zhang and Ghalsasi (2011) introduced four types of stakeholders: consumers, providers, enablers and regulators. Enablers are "those organizations that will sell products and services that facilitate the delivery, adoption and use of cloud computing"; while regulators are those who "pervade across the other stakeholders" (p. 183). The major components and industry players in cloud computing

include: hardware (INTEL, IBM chips to support virtualization); software (VMware, Microsoft,etc.); services (Google, Amazon.com); applications (Software-as-a-Service, or SaaS); virtualization (VMware) or their combination (e.g., Citrix, a classic case of virtualization that merges SaaS and virtualization) (Bento & Bento, 2011).

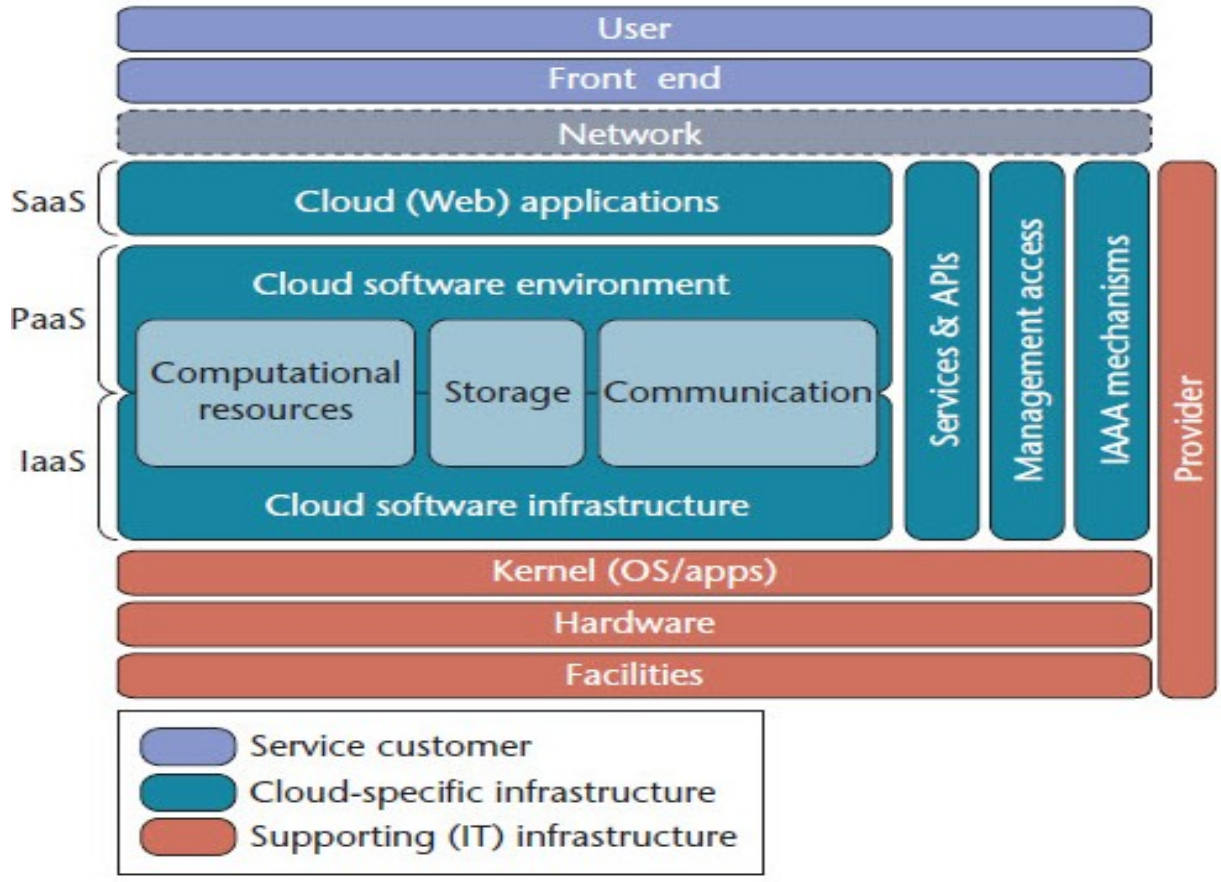

Figure 4: Cloud computing architecture and stakeholders.

Cloud computing brings us both opportunities and challenges. However, if used properly, cloud computing is a technology with great opportunity for businesses of all sizes and types. More and more businesses are taking advantage of cloud computing in many different ways. Xu (2012) stated "Implementing cloud computing means a paradigm shift of business and IT infrastructure, where computing power, data storage and services are outsourced to third-parties

and made available as commodities to enterprises and customers" (p.75). If an organization's data, files, programs, applications are all in the cloud, there is no longer the need for many local machines and hard drives, and massive decentralization becomes possible, as employees just need a netbook, digital tablet, or even a smart phone to store, retrieve and work collaboratively wherever they are: at work, at home, or on the road (Bento & Bento, 2011).

There are numerous advantages of cloud computing for providers, adopters and users. Gupta, Seetharaman and Raj (2013) reviewed some empirical studies on the usage and adoption of cloud computing by small and medium enterprises (SMEs) or small and medium businesses (SMBs) and found that, the most important parameters are: cost reduction, avoiding natural disaster mishaps, sharing and collaboration, trust in cloud providers, reliability, security breaches and service disruption in using cloud computing. They stated "One of the biggest advantages of moving to cloud computing is the opportunity cost of freeing up some of the IT administrative time, which can now be applied to the business aspects of growing the core business of SMBs" (p. 863). Jadeja and Modi (2012) provided five benefits of cloud computing: easy management, cost reduction, uninterrupted services, disaster management and green computing. In addition, Brohi and Bamiah (2011) revealed that cost reduction, easy scalability and increased productivity are the main advantages of applying cloud computing. Accordingly, cost reduction, ease of use and convenience, more productivity, reliability, sharing and collaboration are the highlighted benefits of applying cloud computing.

The advantages excel the organization and business and move to the developmental countries. Also, it meets the need of multiregional branch offices. Cloud computing represents a huge opportunity to many third-world countries that have been so far left behind in the IT revolution (Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011). Cloud computing enables

these countries, which lack resources and professionals, to utilize various and advanced IT services and materials without much need for IT professionals or physical resources. There are various reasons for business, organizations and countries to move towards IT solutions that include cloud computing.

Large enterprises have quickly adopted this cloud computing bandwagon. However, many micro businesses and SMBs are still sitting on the fence and are contemplating whether or not to move to the cloud computing trend. Brohi and Bamiah (2011) stated "According to a survey conducted by International Data Corporation (IDC), 53% of organizations in the Asia-Pacific region are already using some form of cloud computing services, and the remaining 47% of the organizations have plans to adopt private or public cloud services in the next 12 months" (p. 290). Additionally, they revealed that the survey results indicate that cloud computing is a not highly adopted technology; however, the growing contributions by researchers and IT industries will increase the use of cloud computing globally. For several reasons, some organizations and individual users are not yet involved with this innovation of cloud computing.

Armbrust, et.al (2010) described ten top critical obstacles to growth of cloud computing, affecting adoption, growth, business and policy. In summary, these obstacles include business continuity and service availability, data lock-in, data confidentiality/auditability, data transfer bottlenecks, performance unpredictability, scalable storage, bugs in large- scaling quickly, scale distributed systems, reputation fate sharing, and software licensing.

Many studies and researchers have addressed cloud computing threats and other problems that can affect the trust and adoption of the cloud. Security and network challenges within the cloud have become an issue that receives great attention. Lack of privacy and security is the main barrier in the wide adoption to cloud computing. According to Tan and Ai (2011),

"2009 Gartner survey showed that more than 70% of respondents said they do not intend to use the cloud computing at recent, the main reason is afraid of the data security and privacy" (p. 4358). Also, they stated that, a large number of users' files were leaked in Google in March 2009. Aleem and Sprott (2013, as cited in Hutchings, Smith & James, 2013) "interviewed 200 ICT [Information and Communications Technologies] professionals worldwide. Respondents' most cited concern regarding the use of cloud computing was security, as reported by 93.4 percent of interviewees" (p. 2). Martin (2010, as cited in Gupta, Seetharaman & Raj, 2013) found that security and privacy are top concerns of 51% SMBs. In 2009, ICD examined 244 IT executives/CIOs and their line-of business colleagues about their opinions of cloud computing usage; they found that security is the greatest challenge of using cloud computing see Figure5 (Zhang, Wuwong, Li & Zhang, 2010). Therefore, security risk management and solutions within cloud computing should be studied very well and in wide range to address these concerns. It is significant to raise the awareness of applying the newest and most reliable security methods when using cloud computing. Also, it is important to increase the confidence and trust between the users, adopters and providers.

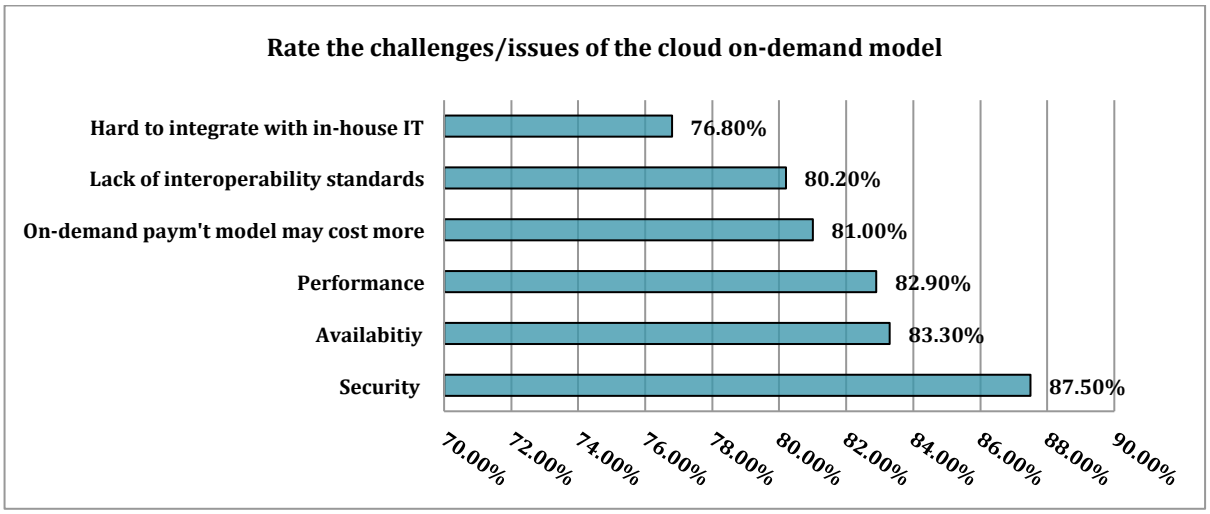

Figure 5: Cloud User Surveys 3Q09 – Security is the "Usual" Challenge.

Finally, cloud computing would change the phase of IT and the way of creating and purchasing software and hardware. In this section, key information regarding cloud computing and its usage has been discussed and reviewed. Security issue within cloud computing has been emphasized. There are many security issues that need to be resolved before cloud computing can be accepted as a viable choice for consumers, providers and business computing. It is obvious enough that adoption of cloud still remains a question mark for some organizations and individual users.

CHAPTER 3

Challenges and Threats

As with any new concept, cloud computing faces several critical issues; the most prominent is the security. As the number of security incidents continues increasing, more people are worried about using the cloud. Many studies and researchers have addressed cloud computing threats and other problems.

Although many cloud computing users tend not to worry about doing backups, keeping hackers out of their data or providing more virtual storage space, there are still various risks that users might not realize. The security of cloud computing is a significant problem in the development of cloud computing. Cloud computing contains important and sensitive data, such as personal, government or business data, that attracts hacker's attention to get the data. Thus, the cloud computing system must be protected carefully with more sophisticated security mechanisms than the traditional computing system. This emphasizes the fact that, traditional security mechanism cannot protect the cloud system entirely (Liu, 2012). Some of the main security problems include data security, user data privacy protection, cloud computing platform stability and cloud computing administration (Liu, 2012). In 2008, "the U.S. information technology research and consulting firm Gartner issued a 'cloud computing security risk assessment' report, mainly from the vendor's point of view about security capabilities and analyzed security risks faced by the cloud. Gartner lists seven major security risks that exists in cloud computing technology" as shown in Table 2 (Tan & Ai, 2011, p. 4358). Cloud computing threats can be divided into two major categories namely: network and security threats. Both will be discussed in this chapter.

Table 2

Seven top security risks

Risk	Description
Privileged user access	Sensitive data processed outside the enterprise brings with it an inherent level of risk
Regulatory compliance	Cloud computing providers who refuse to external audits and security certifications
Data location	The customer probably don't know exactly where your data is hosted
Data segregation	Data in the Cloud is typically in a shared environment alongside data from other customers
Recovery	A cloud provider should tell what will happen to the data and service in case of a disaster
Investigative support	Investigating inappropriate or illegal activity may be impossible in cloud computing
Long-term viability	Data should remain available even after such an event

3.1 Security Threats

As cloud computing users, we lose control over physical security. So, how can we ensure that data will not leak and privacy can be compromised? In order to understand the suggested solutions available, types of attack that we might experience should be highlighted. There are several security threats that occur in cloud computing. Some of which are discussed below:

I. Browser Security: once a user requests a service from cloud server, user's web browser plays a significant role. Even if the web browser uses SSL, sniffing packages on intermediary host

can get decrypted data (Qaisar & Khawaja, 2012). Also, attacker uses decrypted data (credentials) as valid user on cloud system. WS Security (Web Services Security) is a method to eliminate the browser threat by using XML Encryption and XML Signature to guarantee confidentiality and integrity to SOAP messages (Qaisar & Khawaja, 2012). For example, Kerberos, standard usernames and passwords and X.509.

II. Insecure Interfaces and APIs: cloud users are provided with set of software interfaces or APIs to manage the cloud services. Insecure application programming interfaces, which allow software applications to interoperate with each other by passing login information between them, are among the top cloud threats (Hutchings, Smith & James, 2013). "From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy" (Cloud Security Alliance, 2010, p. 9). The big concern with this threat is that third parties often build upon these interfaces to offer value-added services to their customers, which increases the security risks.

III. Cloud Malware Injection Attack: this attack works against cloud services, applications or virtual machines (Hutchings, Smith & James, 2013). Attackers can create their own malicious service by using functionality changes or data modifications for specific purpose (Qaisar & Khawaja, 2012). Then, they upload this spiteful service into the cloud system by tricking the cloud system. Cloud system automatically redirects valid user's requests to the spiteful service implementation, and the malicious code is executed. To prevent cloud malware injection attack, it is necessary to use hash function and to store a hash value on the original service instance's image file and comparing this value with the hash values of all new service instance images (Qaisar & Khawaja, 2012).

IV. Flooding Attacks: this attack exploits some cloud's features, which increases and initializes new services in order to maintain user's requirements and requests. Attacker requests a huge amount of particular service; this means that cloud computing would not be capable to supply service to normal users' requests because cloud system works against the attacker's requests (Qaisar & Khawaja, 2012). DoS Attacks is one type of forceful flooding attacks. According to Qaisar and Khawaja (2012), installing firewall to detect and filter fake requests is a countermeasure for flooding attacks.

V. Data Protection: data protection is very important and complicated for cloud consumer because it is hard to make sure that the data is handled in a lawful way (Qaisar & Khawaja, 2012). For this attack, the consumer should be aware of whither the data is handled in a rightful way or not. In addition, data compromise can occur due to unauthorized parties accesses, loss of an encoding key or deletion or alteration of records without a backup of the original content (Cloud Security Alliance, 2010).

VI. Incomplete Data Deletion: the significant risk that cloud consumer might experience is incomplete data deletion. The reason is that there are many replicas of these data in other servers, maybe as backups. Also, the majority of operating systems do not delete data accurately or completely. Jamil and Zaki (2011 as cited in Qaisar & Khawaja, 2012) revealed that "Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients" (p.1327). Additionally, Qaisar and Khawaja (2012) suggested using VPN and query for securing and completing removing of data from cloud servers that have data replica.

VII. Locks In: the last security issue is locks in. It is related to data, application and service portability. There are little offerings in the way of tools, procedures or standard data formats that could assure data, application and service portability (Qaisar & Khawaja, 2012). Therefore, the cloud customers cannot easily move from one provider to another or shift the services back to an in-house IT environment.

3.2 Network Threats

There are six network issues within cloud computing:

I. Denial of Service (DoS): Denial-of-Service attacks are not new; they can make cloud computing resources and services unavailable to the users (Hutchings, Smith & James, 2013). Overflow frequent requests are sent to the server by attacker to stop the server functionality that provides the services. As a result, the server is unable to respond to the regular users. According to Qaisar and Khawaja (2012), to avoid cloud computing DoS attack, it is important to reduce users/attackers' privileges based on their behaviors when they are connected to cloud server.

II. Man in the Middle Attack: during data transmission between user and cloud server, there is a threat that might occur, called Man in the Middle Attack. According to Hutchings, Smith & James (2013), data that are transmitted in clear without encryption may be hack or stole. Qaisar and Khawaja (2012) suggested encrypting and compressing the data during transmission by installed Secure Socket Layer (SSL) to prevent man in the middle attack.

III. Network Sniffing: it is a kind of analyzing network traffic for hacking unencrypted data that is transmitted through cloud network (Qaisar & Khawaja, 2012; Hutchings, Smith & James, 2013). To illustrate, if the user does not use encryption techniques during the communication

with cloud server, hackers can capture the data such as username and password. Therefore, encryption technique is an effective method to eliminate network sniffing threat.

IV. Port Scanning: attackers use port scanning to discover exploitable communication channels/ports between the user and cloud server. The attacker's goal is to find an active port and exploiting vulnerability of cloud services (Qaisar & Khawaja, 2012). Thus, one of main components of network security structure is firewall. Both user and cloud server need to employ firewall in order to detect and filter authorized traffic.

V. SQL Injection Attack: it is a technique with special character/string to gain unauthorized access or to retrieve information from cloud database (Hutchings, Smith & James, 2013). For example, if the attacker types 1==1 as argument value of query in form field that may retrieve whole database table.

VI. Cross Site Scripting (XSS): it is an attack method to obtain the user's sensitive data (credential) or user's session. Attacker uses a malicious script by web application to redirect the user to the attacker's target (Qaisar & Khawaja, 2012). The script will be activated when it is read by an unsuspecting user's browser or by an unprotected application. For example, login or payment page that is hosted on cloud.com domain; if the attacker discovers XSS vulnerabilities in cloud.com domain, the attacker can use java scripting to steal user's information. Qaisar and Khawaja (2012) stated "Cross site scripting attacks can provide the way to buffer overflows, DOS attacks and inserting spiteful software in to the web browsers for violation of user's credentials" (p.1325).

3.3 Some Solutions for Key Issues in Cloud Computing Security

Tan and Ai (2011) proposed a comprehensive cloud computing security framework (as shown in Table 3) to address some problems in cloud computing security, such as data privacy

and encryption key management. In the infrastructure layer, the confidentiality of data can be ensured through an encryption tunnel technology, ensure from data integrity and non-tampering through digital abstract, and with digital certificates and digital time stamp. According to Tan and Ai (2011), we need host-based firewall, host-based intrusion prevention systems and disk encryption management systems to protect the security of physical devices. We will also need Platform layer associates with access and authentication so data can be protected by verifying user identity utilizing the user fingerprint, passwords and other means.

Table 3

Cloud Security Reference Framework

Application layer	Application	Abuse management	Behavior monitoring	
Platform layer	Data	Data Protection and Leakage Prevent	Data Access Control	Disaster Recovery
	Platform	Governance	Security Management	Authentication
	Virtualization	Virtual Machine Isolation	Virtual Machine monitoring	Access Management
Infrastructure layer	Network	Network Isolation	Traffic monitoring	Origin of attack
	Physical equipment	Firewall	Security Reinforcement	Disk encryption

Common methods for protecting user data include encryption prior to storage, user authentication procedures prior to storage or retrieval and building secure channels for data transmission. These protection methods normally require cryptography algorithms and digital signature techniques, as explained below:

Common data encryption methods include symmetric and asymmetric cryptography algorithms. Symmetric cryptography is used in the U.S. Federal Information Processing Standard's (FIPS) 46-3 Triple Data Encryption Algorithm (TDEA, also known as Triple-DES or 3DES) or 197 Advanced Encryption Standard (AES) and others. This type of encryption and

decryption process uses a secret key. Asymmetric cryptography, on the other hand, uses two different keys, a "public key" for encryption, and a "private key" for decryption. Examples include RSA cryptography and Elliptic Curve Cryptography (ECC). Generally speaking, symmetric cryptography is more efficient, and is suitable for encrypting large volumes of data. Asymmetric cryptography requires more computation time and is used for the decryption keys required for symmetric cryptography (Hwang, Chuang, Hsu & Wu, 2011).

The use of passwords as an authentication process is more familiar to general users, but messages sent by the user are vulnerable to surreptitious recording by hackers who can then use the data in the message to log into the service as the user. In more advanced authentication systems, the system side will generate a random number to send the user a challenge message, requesting the user to transmit an encrypted response message in respond to the challenge message, thus authenticating that the user has the correct encryption key. Without this key, the user will not be allowed access. In the process of challenge and response the client's encrypted key uses the client's password to convert a derived value. In this program, each communication between the client and server is unique, and a hacker using an old message would fail to access the system. In addition, the One-Time Password (OTP) authentication system differs from most peoples' conception of a password. Most people understand a password to be a password chosen by the user to be meaningful, and can be used again and again. The emphasis of OTP however is the single-use nature of the password (Hwang, Chuang, Hsu, & Wu, 2011).

After receiving authentication from the user, the system side must create a secure transmission channel to exchange information with the user. The Secure Sockets Layer (SSL) is a common method of building secure channels, primarily using RSA encryption to transmit the secret keys needed for both sides to encrypt and decrypt data transmitted between them.

When using cryptographic technology to protect user data, the keys used for encryption and decryption of that data must be securely stored. In particular, cloud computing service providers must have specific methods for constraining internal system management personnel to prevent them from obtaining both encrypted data and their decryption keys – this is critical to protecting user data. Operator policies for protecting user data must be clearly laid out in the Service Level Agreement (SLA) and must explain how special privilege users are prevented from improperly accessing user data (Hwang, Chuang, Hsu, & Wu, 2011).

Kandukuri, Paturi and Rakshit (2009) offered six recommendations for SLA content:

I. Special privilege user data access must be controlled to prevent unauthorized storage or retrieval.
II. Cloud computing services must comply with relevant laws.
III. User data must be properly stored and encrypted.
IV. A reset mechanism must be provided in case of service disruption or system crash.
V. Service must be sustainable and guaranteed against service discontinuation due to change or dissolution of the provider.
VI. If cloud computing services are used for illegal purposes, the provider must be able to provide records to assist with investigations.

A common approach to protect user data is that user data is encrypted before it is stored. In cloud computing environment, a user's data can also be stored following additional encryption. But if the storage and encryption of a given user's data is performed by the same service provider, the service provider's internal staff (e.g., system administrators and authorized staff) can use their decryption keys and internal access privileges to access user data. From the

user's perspective, this could put his stored data at risk of unauthorized disclosure.

Creating user trust through the protection of user's data content is the key to the widespread acceptance of the cloud computing. Hwang, Chuang, Hsu and Wu (2011) proposed a business model for cloud computing based on the concept of using a separate encryption and decryption service. In the model, data storage and decryption of user data are provided separately by two distinct providers. In addition, those working with the data storage system will have no access to decrypted user data, and those working with user data encryption and decryption will delete all encrypted and decrypted user data after transferring the encrypted data to the system of the data storage service provider.

Under the business model proposed in Hwang's study, the data storage cloud system provider is authorized to store the user's encrypted data, but does not have access to the Decryption Key. Thus, the storage system can only retrieve encrypted user data, but is unable to decrypt it. The cloud computing system responsible for encrypting user data has authority over all encryption keys required for data encryption but, given that the encryption provider does not store the user's data, internal mismanagement of the decryption keys still poses no risk of unauthorized disclosure of the user's data. Given that encryption is an independent cloud computing service, a unique feature of the business model is that different services are provided by multiple operators. For example, the Encryption as a Service provider and the "Storage as a Service" provider cooperate to provide a Cloud Storage System with effective data protection. This study provides a draft SLA for this type of business model of combining multiple providers in a single service, which can establish the cooperation model between operators and the division of responsibility for the services they jointly provide to the user (Hwang, Chuang, Hsu, & Wu, 2011).

However, data encryption cannot protect the data completely with respect to rogue administrators because encryption keys stored or used on cloud systems are subject to eavesdropping (Claycomb & Nicoll, 2013). Several methods have been suggested to protect data in the cloud. According to Claycomb and Nicoll (2013), there are novel solutions to protect data in the cloud, but these are clearly not the only options proposed for secure data storage in the cloud. One is to "simply store and/or transfer encrypted information, without introducing the associated keys to the cloud system, is a potential way to protect that data from a rogue cloud administrator" (p. 4). Hutchings, Smith and James (2013) provided several ways to prevent crime and security attacks (as shown in Table 4).

Table 4

Summary of cloud computing crime and security prevention measures.

	Technical prevention measures						Physical security					Organisational policies, awareness and training					
	Patching operating systems, internet browsers and software applications	Installing anti-virus, anti-malware tools and firewalls	Implementing multifactor authentication	Encrypting data travelling between the cloud and the browser	Encrypting data stored in the cloud	Intrusion detection and prevention systems and network monitoring	Perimeter security	Shielded server rooms and cages	Surveillance	Access control	Facility access logs	ICT-acceptable use policies	Password policies	User access management policies	BYOD policies	Staff training	Background checks of cloud service provider staff
Crime and security risks involving cloud service providers																	
Authentication issues		✓	✓		✓	✓						✓	✓	✓	✓	✓	
Denial of service attacks and botnets		✓				✓											
Use of cloud computing for criminal activities						✓											
Illegal activity by cloud service providers					✓												✓
Attacks on physical security					✓		✓	✓	✓	✓	✓						
Insider abuse of access			✓		✓	✓			✓	✓	✓						✓
Malware	✓	✓	✓		✓	✓						✓			✓	✓	
Side channel attacks					✓												
Vulnerabilities in software applications	✓	✓	✓		✓	✓						✓					
Cryptanalysis of insecure or obsolete encryption					✓												
SQL injection	✓	✓			✓	✓											
Crime and security risks targeting cloud computing tenants																	
Phishing			✓		✓							✓	✓			✓	
Domain name system attacks	✓		✓		✓							✓	✓			✓	
Compromising the device accessing the cloud	✓	✓	✓		✓	✓						✓	✓		✓	✓	
Access management issues			✓											✓			
Attacks targeting the transmission of data																	
Session hijacking and session riding				✓													
Man-in-the-middle attacks				✓													

CHAPTER 4

Risk Management Framework

In this thesis, a risk management framework is suggested for cloud computing providers regardless of their types and models based on NIST risk management guide and McGraw's security risk management. From a business perspective, cloud computing providers were basically found to provide products and services and for their own profits.

Among various ways to deliver computing resources and services, a cloud computing provider is one of the best self-services on Internet infrastructure. Cloud computing provider's underlining mission is that every user can utilize available applications and get services easily regardless of their locations and the underlying operating system of their devices. Their business goal is to deliver high secure and reliable applications and services. Also, they aim to gain costumer's trust and loyalty.

Cloud computing providers have encountered dangerous security risks and problems. These issues would affect negatively confidentiality, privacy, reliability and integrity of providers' services. Therefore, a specific risk management process called Risk Management Framework (RMF) of dealing with security risks and problems within computing aspect is recommended. The basic idea of RMF is simply "identify, rank, track, and understand software security risk as it changes over time" (McGraw, 2006, p. 54). This framework can be used in wide range and flexibility because it can fit both small and large enterprise. Also, "RMF is not specific to security risks; it can be applied in non-software situations" (McGraw, 2006, p. 56). The main goal of providers using RMF in cloud computing is to consistently track and handle risks.

It is important to define risk management and its purpose in general. Stoneburner, Goguen and Feringa (2002) defined risk management as "the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions" (p.11). The explicit goal of applying risk management in any organization is to minimize negative impacts on organizations and need for sound basis in decision making.

4.1 Risk Management Processes Enable an Organization to Discover and Assess Its Risks and to Determine How to Control or Mitigate the Risks as Follows:

4.1.1 Risk identification

Risk identification is the process of finding out the incidents that may cause damages to information systems and associated business processes. A according to International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC) 13335-3, we can use the following approaches to identify risks: In the baseline approach, an organization knows its deficiencies by comparing its current security safeguards to the minimum safeguards suggested by security standards or code of practices. For example, Karabacaka and Sogukpinarb (2006) evaluated the risks of an organization based on the degree of compliance with ISO 17799; the informal approach allows people exploiting their knowledge and experience to list the risks. For example, CORAS provides a UML-based approach for people to model and analyze the risks during brainstorming. The detailed risk analysis approach involves in-depth reviews of information systems in an organization; finally, the above combined approaches are used hybridly. For example, people in an organization can determine the critical information systems informally. Then, the detailed risk analysis approach is used to identify the potential incidents to critical systems. For the other systems, the baseline approach is used.

4.1.2 Risk assessment

Risk assessment is to predict impacts of the identified potential incidents through quantitative or qualitative approaches. Quantitative approach usually evaluates the potential loss of incidents by monetary values. The most representative quantitative scheme is incident by multiplying the frequency of the incident occurring within a year (which is usually referred to as the annualized rate of occurrence (ARO)) with the most likely loss from the incident (or the single loss expectancy (SLE) of the incident). Instead of trying to assign monetary values to risks, qualitative scheme, such as OCTACE, ISRAM, CRAMM, and so forth, evaluate the risks by relative levels. In general, the qualitative scheme is easier to be executed and understood by people who are not experts on security or computers than the quantitative scheme. However, organizations can use the monetary results of quantitative scheme to calculate the return of security investment and to decide the amount to insure directly.

4.1.3 Risk treatment

Once a potential incident has been identified and assessed, an organization needs to decide how the risk is to be treated. Possible options include:

(1) Doing nothing and accepting the risk.

(2) Avoiding the potential incidents by changing or terminating associated actions or business processes.

(3) Having insurance or transferring the risks to other parties.

(4) Applying appropriate security safeguards to mitigate the risks to an acceptable level. There are several kinds of safeguards. If more than one option of security safeguards can be applied to the same potential incident, an organization can use cost-benefit analysis or other approach to optimize its security investment. The issues are out of scope of this article.

4.1.4 Monitoring and re-assessing the risks

The residual risks and identified acceptable risks should be regularly monitored and reviewed to ensure the correctness and effectiveness of risk assessment and treatment. In addition, an organization may need to re-assess its risks to reflect major changes to the organization (Cha, Juo, Liu & Chen, 2008).

Tanimoto, Hiramoto, Iwashita, Sato and Kanai (2011) analyzed cloud computing security problems in detail on the basis of the risk breakdown structure (RBS) method and the risk matrix method. They provided risks that extracted from user's viewpoints. Xie, Peng, Zhao, Chen, Wang and Huo (2012) suggested a risk management framework for cloud computing, which consisted of five components: user requirement self-assessment, cloud service providers desktop assessment, risk assessment, third-party agencies review, and continuous monitoring. Our framework is different in that Xie, et. al involved users, providers and third party in their framework. While, we emphasize the business angle in this framework; the marriage of business and technical concerns is the central drive to our risk management plan. Also, increasing the adopters and users of cloud computing is one of this framework goals. For cloud computing to spread, users must have a high level of trust in the methods by which service providers protect their data. Our RMF consists of six stages, which will be discussed in detail later in the next section. While, other frameworks consist of five stages or less. In order to minimize the impacts associated with cloud computing concerns, risk mitigation is imperative if organizations want to take advantage of the many benefits of cloud computing while protecting and safeguarding systems and data. Management is under pressure to ensure adequate mitigation of risks to reduce the impact on business.

4.2 RMF Stages

The RMF consists of six fundamental activity stages namely (1) understand the business context, (2) identify the business technical risk, (3) synthesize and prioritize the risk, (4) define the risk mitigation strategy, (5) carry out required solutions and validate that they are resolved and (6) overall assessment and monitoring of the system Each stage is discussed in detail below:

4.2.1 Understand the business context

This includes describing business's goals, priorities and circumstances in order to understand what kinds of software risks to care about and which business goals are paramount. The main purpose of this stage is to gather data to answer the all-important "Who cares?" question.

4.2.2 Identify the business, technical risks and their vulnerabilities

The business risks can impact business goals. For example, these risks can have impact on business reputation, revenue, productivity and others. The identification of business risks helps to define and choose the most effective technical and managerial methods for measuring and mitigating these risks. In terms of technical risks, they are hard to find because they are often not obviously interacting. They can be related to a system behaving in an unexpected way, violating its own design structures, failing to perform as required or process of building software.

4.2.3 Synthesize and prioritize the risks, producing a ranked set

In any system, large number of risks will always exist. In this stage, the prioritization process must consider the most important business goals and which goals are immediately threatened. Some questions that should be answered in this stage: "what shall we do first given the current risk situation? What is the best allocation of resources, especially in terms of risk mitigation activities?" (McGraw, 2006, p. 59).

4.2.4 Define the risk mitigation strategy

In this stage, a coherent strategy should be created for mitigating the risks in a cost-effective manner. "Any suggested mitigation activities must take into consideration cost, implementation time, likelihood of success, completeness and impact over the entire corpus of risks" (McGraw, 2006, p. 59).

4.2.5 Carry out required solutions and validate that they are resolved

This stage involves carrying out the validation techniques, which provides confidence that risks have been properly mitigated through artifact improvement and that strategy is working. Also, the mitigation strategy should be tested to make sure it is effective.

4.2.6 Overall assessment and monitoring stage

After carrying out the required solution, the teams of experts meet to continually evaluate and assess the outcome of the applied solution. Based on observations, the team decides whether the risk assessment meets the plan or not and what they should do next in each situation. If the risk assessment meets the plan, they can document the type of attach/threat and the effective solutions. They can then think of the vulnerabilities of the solution and ways to fix them. Besides, alternative solutions can also be devised to increase readiness should the current solution fail in the sight of a similar attack. The experts can also evaluate the performance of the solution to see the effectiveness in meeting the goals of the business partners as well as securing the confidence of their clients. If the solution fails, the experts can assess why the solution failed and come up with ways to fix it. They can evaluate the extent of damage and come up with effective ways of counteracting any aftermath of such attacks. They can also embark on effective ways of restoring the confidence of their clients should the attack tamper with their data security or privacy information. This team of experts form the backbone of cloud computing because

their innovative thinking dose not only provide robust mechanisms for combating known threats but also provides the platform for developing more effective and dynamic RMF. Since humans are the most dangerous potential threat source, a team providing great monitoring and performing continuous and combating procedures is indispensable to any reliable risk management framework.

4.3 Discussion

A continuous risk management process is a necessity in cloud computing. Also, continuous monitoring process is required through ongoing risk identification, implementation and assessment. The risk management plan should be well organized, which requires collaboration between and among different departments. Sufficient time must be given for planning, organizing, collaboration and communication.

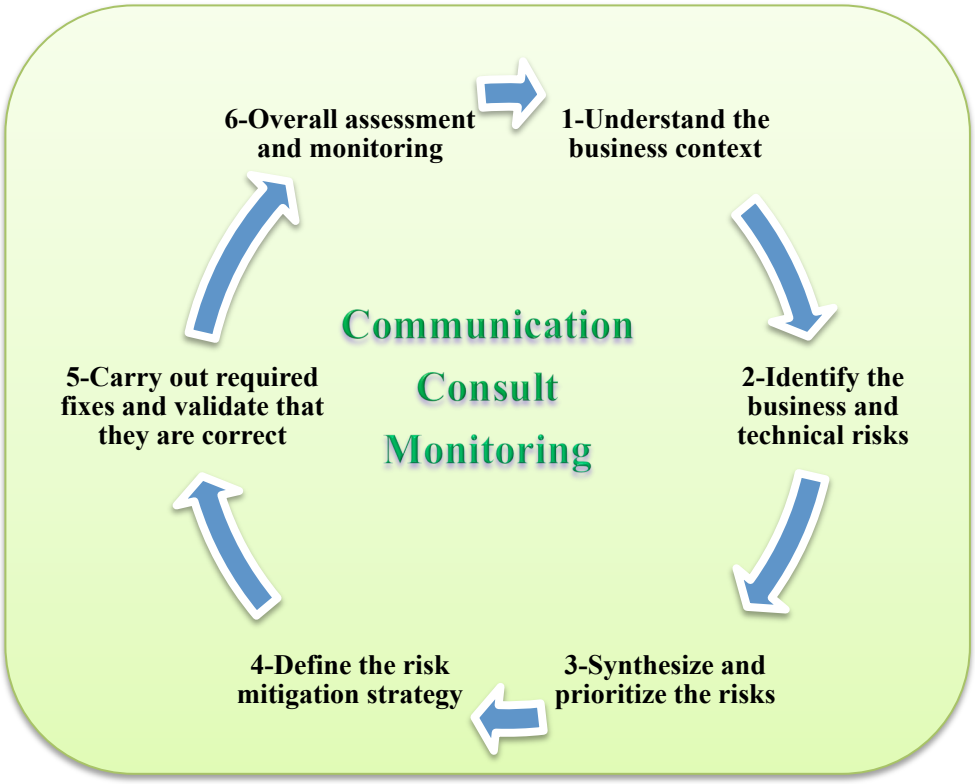

Figure 6: The RMF consists of six fundamental activity stages

Figure 6 above shows in the middle that monitoring is needed all the time in the entire process to make sure what was expected is actually working. This needs to be performed at consistent time intervals set in the risk management documentation. Sometimes it is necessary to place a watch on areas and at other times it will be prudent to change a certain process. If the process has been changed it gets added to your risk management documentation. Some organizations prefer to outsource the monitoring and others will keep the monitoring in-house. When monitoring cloud services it might be logical to form a team between several different companies to better form mobility in the documentation.

Also, in the middle of Figure 6, it states communication and consulting. This implies that we should keep all stakeholders informed of what the risk management documentation states and if it changes you will need to contact all those stake holders. This is why outsourcing of monitoring is currently popular in the cloud. Small businesses lack the resources to deal with constantly talking with stakeholders while monitoring their systems.

In the first stage, which is the preparation for risk assessment and identification, different information including quantitative and qualitative data will be gathered. System analysts should develop several questions to interview and survey different people (e.g manager, IT management, clients, developers, employees). These questions can address (but not limited to) business goals and mission, average new and leaving clients per a month, business profile and functions, profit average, advertising and marketing, resource suppliers, client claims, current technical defects and defense methods, system need to support several languages, service interruption during system maintenance, and system backups. Also, they are encouraged to develop research project to examine the overall system and decompose it into reasonably small set of components. Also, choosing relevant critical areas to focus on is necessary; especially the

area needs immediate attention. Table 5 (NIST's rough guidelines for ranking business goals can be used) provides a guideline for ranking goals in a way that effectively meet standards required by federal regulations. This ranking places business goals under three broad heading of High (H), Medium (M) and Low (L) depending on the extent of its impact on the project, the employees and the company at large. The goal is ranked high if it is crucial to the existence and continuity of the project. Failure of such goals has the potential to halt the entire project and directly impact the company. Medium ranked goals are crucial to the existence of the project and their failure may adversely affect many employees and also impart some high ranked goals. Failure of low ranked goal can affect just a small portion of the company's revenue and the impact may be felt by just a small portion of the company's employees.

Table 5

Guidelines for business goals rankings from NIST

Rank	Definition
High	These goals are critical to the existence of the project (and possibly the company). If these goals are not met, there is a real risk that the project will cease to exist and the company will be directly impacted.
Medium	These goals are very important for the existence of the project (and possibly the company). A large number of emploees may be affected if these goals are not met. A failure to achieve a mediume-rank business goal may result in a negative affect to high-rank goals.
Low	These goals affect only a small portion of the company's revenue. A small number of employees may be affected if these goals are not met.

Creating risk management plan's directions, committees, goals, requirements, timeline and scope is required to do in the beginning. The goal for doing this is to ensure that everyone in the committees is aware of his/her responsibility, role and time they have. Also, it would make the efforts spend more effective and direct.

The second stage includes risk analysis and assessment. When identifying the business and technical risks, three fundamental sources of threats should be taken into account: natural (e.g. floods, earthquakes, tornadoes), human (including unintentional acts and deliberated actions such as network based attacks) and environmental threats (e.g. Long-term power failure, pollution, chemicals). The most prominent among these categories is the human attackers. The motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources. Table 6 outlines many of today's common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack (McGraw, 2006).

Also, these sources can be dividing into two broad categories namely adversarial incidents and non-adversarial incidents (Feng Xie, 2012). The adversarial incidents are those initiated by mainly human adversaries such as hackers and cybercriminal organizations. While, the non-adversarial incidents occur due to environmental problems such as the earthquake, flood, system fault, or are initiated by unintentional operators.

In stage two, technical, managemental and operational vulnerability should be searched too. Applying vulnerability sources, the performance of system security testing, and the development of a security requirements checklist can help identifying system vulnerabilities. The output of this process helps to identify vulnerabilities and threats for reducing or eliminating risk during the risk mitigation process.

Table 6

Human Threats: Threat-Source, Motivation, and Threat Actions

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)

Table 6

Cont.

Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

After the deduction of risks and vulnerability, risk indicators, impact of risks and likelihood of identified risks to be occurred must be created (see Table 7 & 8). Table 7 can be used for calculating the risk occurrence likelihood of both the adversarial and the non-adversarial incidents as highlighted in the literature. Here, the categories that can be identified with various degrees of risk are tabulated and explained. Table 8 gives a similar metric but in a much compressed and simplified form. The likelihood of an incidence can be modeled as the maximum of the likelihood of the adversarial incidence and the likelihood of the non-adversarial incidence. Risk indicators are signs and important tool within operational risk management that can be used to monitor and measure by the analyst to determine the status of risks over time. Table 9 outlines the business impact scale provided by NIST. It categorizes the impact into High, Medium and Low and explains the extent of each impact. The more likely the incidence is

to occur and a consideration of the adverse impact can be used as a major risk assessment indicator by the business. The level of impact and the likelihood of occurrence would allow the analyst to evaluate the impact of business risk on different business goals (see Table 10) (McGraw, 2006). In addition, this step involves discovering and describing technical risks and linking them to business goals.

Table 7

The occurrence Likelihood levels of cloud security incidents

Levels	Meaning	Types	Description
4	Very High	A	The incident is almost certain to be initiated by adversary
		NA	The incident is almost certain to occur, or occur more than 100 times a year
3	High	A	The incident is highly likely to be initiated by adversary
		NA	The incident is highly likely to occur more between 10- 100 times a year
2	Medium	A	The incident is somewhat likely to be initiated by adversary
		NA	The incident is somewhat likely to occur, occur more between 1-10 times a year
1	Low	A	The incident is unlikely to be initiated by adversary
		NA	The incident is unlikely to occur, or occurs less than once a year, but more than once every 10 years
0	Very Low	A	The incident is highly unlikely to be initiated by adversary
		NA	The incident is highly unlikely to occur, or occur less than once 10 years

Table 8

NIST risk likelihood description

Likelihood Value	Definition
High	The threat is highly motivated and sufficiently capable, and controls to prevent the risk from occurring are ineffective.
Medium	The threat is motivation and capable, but controls are in place to impede successful materialization of the risk.
Low	The threat lacks motivation or capability, or controls are in place to prevent or at least significantly impede the risk from occurring.

Table 9

NIST business impact scale

Business Impact Value	Definition
High	1. Very costly loss of major tangible assets or resources. 2. Significant violation of, or harm or impediment to, an organization's mission, reputation, or interest. 3. Human death or serious injury.
Medium	1. Costly loss of tangible assets or resource. 2. Violation of, or harm or impediment to, an organization's mission, reputation, or interest. 3. Human injury.
Low	1. Loss of some tangible assets or resource. 2. A noticeable effect on an organization's mission, reputation, or interest.

In order to understand and manage risks, analysts must establish relationships between the business goals, business risks and technical risks. It is helpful to draw visual relationship between business goals, business risk and technical risk. It is possible that an individual technical

risk may impact multiple business goals at different severity levels. Additionally, analysts are strongly encouraged to prioritize these goals and risks in meaningful business terms.

Table 10

Risk scale – level of risk in relation to likelihood and impact

Likelihood (threat event occurs and results adverse Impact)	Impact		
	Low 10	Moderate 50	High 100
High (1.0)	Low 10*1.0 = 10	Moderate 50*1.0=50	High 100*1.0=100
Moderate (0.5)	Low 10*0.5=5	Moderate 50*0.5=25	Moderate 100*0.5=50
Low (0.1)	Low 10*0.1 =1	Low 50*0.1=5	Low 100*0.1=10

Note: risk scale= high (50.1 to 100); moderate (10.1 to 50); low (1 to 10).

In the third stage, synthesize and prioritize the risks, producing a ranked set, analysts can develop the technical risk severity by business goals and how each technical risk impacts on business goals (see Table 11). To determine the severity level, likelihood of technical risk occurrence and business impacts must be assessed. So, based on all the information gathered so far, management team is able now to create the outline for risk mitigation strategy.

At fourth stage, define the risk mitigation strategy; coherent strategies should be created taking into account their effectiveness. Also, the management team should answer the question "How can the identified risks be managed?" Different mitigation methods should be proposed to

Table 11

Level of risks

Quality Values	Semi-Quantitative Value		Description
Very High	96-100	10	Very high risk means that a threat event could be expected to have multiple severe or catastrophic advance effects on organizational operations, organizational assets, individuals, other organization, or the Nation.
High	80-95	8	High risk means that a threat event could be expected to have a severe or catastrophic advance effects on organizational operations, organizational assets, individuals, other organization, or the Nation.
Moderate	21-79	5	Moderate risk means that a threat event could be expected to have a serious advance effects on organizational operations, organizational assets, individuals, other organization, or the Nation.
Low	5-20	2	Low risk means that a threat event could be expected to have a Limited advance effects on organizational operations, organizational assets, individuals, other organization, or the Nation.

Table 11

Cont.

Very Low	0-4	0	Very low risk means that a threat event could be expected to have a negligible advance effects on organizational operations, organizational assets, individuals, other organization, or the Nation.

Note: 0 to 10 = risk rating (0 = very low and 10= very high); 0 to 100 = value.

choose the best and the most effective one that make sense economically and can cover many risks. The method that provides large risk coverage at low cost should be considered. Also, several issues should be taken into account when selecting mitigation methods such as legislations, regulation, organizational policies and impact of method implementation on operations. After that, a completed risk analysis report should be ready to present for management team and peer review.

In the fifth stage of RMF, carry out required fixes and validating, involves implementation process and application of validation techniques. Validation plan and instruments are different from one project to the other based on risk identified and methods choosing to address them.

At the last stage, overall assessment and monitoring stage, all teams have to meet frequently and at the end of the process to assess their works, decide if the risk assessment meet the plan or not and what they should do next in each situation. The purpose is to be able to detect and address any problems that need more attention or those that have just come up through the process.

In business and technology fields, mentoring is a good way of efficiently transferring valuable competencies from one person to another or from one group to another. This would expand the organization's skills base and help to build strong teams.

There are several skills that should be emphasized in this stage to assure a successful assessment and monitoring. The assessment and monitoring team should have the desire to help and spend time helping others. They should remain positive throughout and be motivated to continue developing and growing. Asking the right questions is important in the assessment stage. To do this, assessment team should try asking open questions that cannot be answered with just yes or no. Or ask more direct questions that offer several answer options. Then ask why they chose that particular answer. Also, they should listen carefully and actively to all other involved teams and individual. Finally, providing comprehensive feedbacks is the most important skill needed in this stage. It would help fixing and detecting all problems occurred. Also, it can improve the work and its progress.

4.4 How to Use the Framework (A Scenario Explaining a Step-By-Step Approach to Applying a Risk Management Framework to a Hypothetical Cloud Computing Provider)

This section is an example to apply information security risk management framework for the cloud computing to identify and manage risks. We used a hypothetical cloud computing provider. The framework has six stages: Understand the business context; Identify the business, technical risks and vulnerability; Synthesize and prioritize the risks; Define the risk mitigation strategy; Carry out required fixes and validate that they are correct; Overall assessment and monitoring. Each process will be necessary to clarify specific roles, responsibilities, and accountability for each major process step.

I. Understanding the business context: the provider, CloudPro, is a private one. CloudPro's business goals are to provide private cloud services and deliver the security, availability and reliability for the business applications that will use these services. CloudPro system is made up of a network of computers that utilize virtualized resources in order to better handle workload. User can access cloud application and services through a web browser (interface software) while the applications and data are stored on CloudPro cloud servers. There are technical and operational controls that CloudPro currently uses to detect and prevent software risk. Firewall is used to block external and internal users from accessed information that has been blocked by the specified client/organization/company. Access control mechanisms controls the level of access granted to each user. Each user can have unique security authorizations, eliminating the need for shared passwords or keys and that will control information privilege. Cryptography, user can have the data and objects they store in CloudPro cloud encrypted automatically using Advanced Encryption Standard (AES). Also, our client can establish secure and encrypted communication sessions using SSL. During interview, we found some significant information that can help to track uncovered risks. First point that we got from the manager was clients' claims about data security and privacy. Also, there were some disconnected services during a day, approximate one each month. That affected CloudPro's annual income and caused a decrease in the number of clients. Based on preliminary investigation with software developer, we found some malicious code within CloudPro cloud's applications that caused storage failures. A good point that we found and can help is firewall. Attackers use port scanning to discover exploitable communication channels/ports between the user and CloudPro's cloud server. The attacker's goal is to find an active port and exploiting vulnerability of cloud services. Thus, one of the main components of network security structure that we built is firewall. Both user and CloudPro's

cloud server have employ firewall in order to detect and filter authorized traffic. According to software developer interview, we extracted that user's web browser plays a significant role once a user requests a service from CloudPro's cloud server. To eliminate browser threat, CloudPro's cloud server used XML Encryption, such as Kerberos, and XML Signature to guarantee confidentiality and integrity services. Based on manager answers, CloudPro's cloud server needs new security requirements in order to prevent and avoid incomplete data deletion, since there are many replicas of clients' data in other servers as backup.

II. Identify the business, technical risks and vulnerability: the three main business goals in CloudPro are availability, high security and privacy, and sustainability. Here is the list of risk discovered: Distributed Denial of Service (DDoS) attack on cloud computing; Security weaknesses cause service and storage failures; Identity and access control are failed to control threats and vulnerabilities during communication sessions. Description of each risk can be found in Appendix A.

III. Synthesize and prioritize the risks: CloudPro's ranked goals, business risks, full set of business risk data tables are shown below. CloudPro analyst can conclude that the availability of the project's goal is fully imparted by DDoS attack; security weaknesses. That Distributed Denial of Service (DDoS) attack reduces system reliability; security weaknesses cause service and storage failures; identity and access control are failed to control threats and vulnerabilities during communication sessions. Besides, DDoS and fault tolerance testing feeds the business risk of unplanned downtimes (see Table 12). The CloudPro analyst concludes that DDoS and TR1 imparts the most important goals of the project since the risks possess high likelihood of occurrence and if the failure continuous, it will affect the reliability of the system and compromise their security of the business clients(see Table 13). It however has no impact (N/A)

on availability of service but has low impact on the sustainability and longtime reliability of the project. Complete tabulation as shown in Table 13 which links the severity of the technical risk with the business goals, the cloudPro analyst indicates the most severe technical risks that requires urgent attention and must be addressed by the project to meet business high priority business goals. This possess critical information that will aid the decision making such as those needed to ensure maintenance, security improvements, etc. This is crucial to the Risk Management Framework.

Table 12

CloudPro Goal-to-Risk Relationship

Business Goal	Business Risk	ID #	Technical Risk
Availability	Flooding a network interface with attack traffic in order to overwhelm its resources.	TR 2	Cloud provider malicious insider.
		TR 3	Compromise Service Engine.
Security & Privacy	Security weaknesses cause service and storage failures.	TR 1	Data Protection Risks.
		TR 2	Cloud provider malicious insider.
		TR 3	Compromise Service Engine.
	Identity and access control are failed to control threats and vulnerabilities during communication sessions.	TR 2	Cloud provider malicious insider.
		TR 3	Compromise Service Engine.
Sustainability	Security weaknesses cause service and storage failures.	TR 1	Data Protection Risks.

Note: TR= Tier (TR1=Organizational level; TR2= Mission, business process level; TR3= Information system level).

Table 13

CloudPro Technical Risk Severity By Business Goals

ID #	Technical Risks	Business Goal		
		Availability(H)	Security & Privacy (M)	Sustainability (M\L)
TR1	Poor control access and CloudPro's cloud management caused data protection risks.	N/A	H	L
TR 2	Compromise Service Engine.	H	H	N/A
TR 3	Cloud provider malicious insider during when attacker use CloudPro's services.	H	H	N/A

Note= H= high; M= medium; L= low

The CloudPro then designs the risk mitigation strategy (see Table 14). The type of methodology adopted depends on the type of business risk being considered. The table gives examples of the business risks that can be encountered and suggested mitigation strategy for each of these risks. These strategies take into consideration the top goals of the business and how the various business risks affect these goals as against the cost of mitigation. Business risks with high likelihood of occurrence and great impact on the business goals (business goals) are given more resources and attention since their mitigation is considered a great business accomplishment.

The business goals of CloudPro (see Table 15) are outlined and clearly explained. These include: availability (rank M) - CloudPro cloud must ensure that their client resources and services remain continuously available. The requirement is fundamental to keeping the trust of there

Table 14

CloudPro Recommended Risk Mitigation Methods

Business risk	Supporting technical risk	Risk mitigation methods			
		Add cloud risk readiness and operations	Add security requirements and security requirements	Additional Team Training	Audit Controls
Flooding a network interface with attack traffic in order to overwhelm its resources and deny it the ability to respond to legitimate traffic.	TR 1	H	M	H	M
Security weaknesses cause service and storage failures.	TR 2	H	H	H	M
Identity and access control are failed to control threats and vulnerabilities during communication sessions.	TR 3	M	H	H	M

clients as well as ensuring the provision of services anywhere and anytime to meet SLA requirements; Security & Privacy – This is to guarantee that user applications and data are being protected by highly secure facilities and infrastructure; and Sustainability: This focuses on data center efficiency and server utilization, by utilizing advanced data center infrastructure will design that reduce power loss through improved cooling and power conditioning.

Table 15

CloudPro Business Goals

Rank	Business goals	Description
M	AVAILABILITY CloudPro cloud must ensure that their client resources and services remain continuously available.	Since CloudPro has been improved rapidly and used in wide range, CloudPro must provide 99.99% services anywhere and anytime to meet SLA requirements.
M	SECURITY & PRIVACY CloudPro must guarantee that user applications and data protected by highly secure facilities and infrastructure.	CloudPro cloud must work to provide optimum security while ensuring complete customer privacy to keep their customers and to comply with the Data Protection Act 1998 (DPA)
M/L	SUSTAINABILITY CloudPro's should focus on data center efficiency and server utilization, by utilizing advanced data center infrastructure will design that reduce power loss through improved cooling and power conditioning.	It will positively impact employee satisfaction and customer confidence and lead CloudPro to achieve Global Data center and Cloud Award for best improvement process for energy efficiency in the data center.

The CloudPro business risks are also tabulated and used for the decision making (see Table 16). These business risks include flooding a network interface with attack traffic in order to overwhelm its resources and deny it the ability to respond to legitimate traffic; Security weaknesses cause service and storage failures; and Identity and access control are failed to control threats and vulnerabilities during communication sessions.

A more comprehensive set of business risk data for CloudPro has been tabulated on Table 17. Note that this outlines Business Risk, Business Risk Indicators, Likelihood, Impact,

Estimated Cost, Impact, Severity and Risk Mitigation methods and cost considerations. It holds more information necessary for making inform decision.

Table 16

CloudPro Cloud Computing Business Risks

Business risks	Description
Flooding a network interface with attack traffic in order to overwhelm its resources and deny it the ability to respond to legitimate traffic.	Distributed denial of service (DDoS) and other attack will impact negatively on business availability. If these attack succeed will hardly stop the negative effects. It will lead to lose our clients and their trust. CloudPro will spend a lot of its resources to retrieve cloud services and clients confidence.
Security weaknesses cause service and storage failures.	CloudPro may harm their clients without knowing. A professional attacker (as user) can install malicious code when he use an application then another user may use this particular application. These malicious codes can damage both cloud services and user tools. Also, user data can be changed or stolen and publish in the public. News about the failure of security can destroy CloudPro reputation.
Identity and access control are failed to control threats and vulnerabilities during communication sessions.	The failure of the control privilege affects users' privacy and cause right issue. Stealing valid session even if the content is encrypted, the attacker pretends to be legitimate user and he can prevent legitimate user from using the system.

Also, the impact of the cloudPro's technical risks (see Table 18) is considered in this RMF. The impact of technical risks such as Data Protection Risks, Compromise Service Engine, Cloud provider malicious insider are important to decision makers.

Table 17

CloudPro Full Set of Business Risk Data

Business Risk	Business Risk Indicators	Likelihood	Impact	Estimated Cost	Impact	Severity
Flooding a network interface with attack traffic in order to overwhelm its resources and deny it the ability to respond to legitimate traffic.	Slow network performance.	H	CloudPro users are unable to access and reach their services and information.	Revenue loss:10 Million. Market share loss: 35% Services and reputation damage:	H	H
Security weaknesses cause service and storage failures.	User has trouble during store data and bugs during working in applications.	M	CloudPro will be unable to meet its users' requirement.	Revenue loss: 4.5 Million Market share loss: 8% Services and reputation damage: extreme Regulatory violation.	M	M
Identity and access control are failed to control threats and vulnerabilities during communication sessions.	User can note some changes and last activity time or he cannot access into his account.	M	CloudPro will be unable to meet its users requirement and non-comply with the Data Protection Act (DPA).	Revenue loss:1 Million Market share loss: 3% Services and reputation damage: limited Legal risk Extreme Regulatory violation.	M	M

Table 18

Impacts of CloudPro's Technical Risks

ID #	Technical Risk	Technical Risk Indicators	Likelihood	Impact
TR1	Data Protection Risks.	There may be security breaches that are not notified by the cloud provider. Loss of control of the data processed by the cloud provider. There is an obvious increment in case of multiple transfers of data.	High	Personal sensitive data. Customer trust. Company reputation.
TR2	Compromise Service Engine.	Cloud provider may receive data that not lawfully collected by its customer. Service engine code vulnerabilities prone to attack by hackers (hacking). Unexpected failure in the service engine. Reduce in the resources assigned to customers.	M	HR data. Service delivery\real-time services. Personal data – critical
TR3	Cloud provider malicious insider	Unclear roles and responsibilities. Inadequate physical security procedures. Poor management.	M	Company reputation. Customer trust. Personal data. Confidentiality, Integrity and Availability.

IV. Areas to ensure that CloudPro's customers have confidence in the cloud: availability, security and compliance, privileged user access, and data protection.

1. Availability:

   Availability is the greatest risk (McGraw, 2006). Understanding the infrastructure of the cloud and avoiding single point of failure are required. Private clouds might reduce the availability risk but add more cost (Xie, et. al, 2012). We can balance the risk by using multiple data centers with the risk of a single suite failure.

2. Security and compliance, privileged user access:
   - Support to HR and data policies 24/7.
   - Evaluating for access control.
   - Encryption of Data.
   - Understanding liabilities.
3. Data Protection:
   - Encryption of Data.
   - Understand "How, Where, When" of customer data storage.
   - Proper Data backup.
   - Understand backed up systems.
   - Identify the time required for full recovery.
   - Practice of full recovery to test Cloud Service Provider's response time.

V. Carry out required fixes and validate that they are correct: DDoS attacks can cost businesses sales, customer loyalty and search engine rankings. However an attack on unprepared business result in few days downtime and not functioning properly. But having a solid DDoS response plan as part of our company's business is essential for the wellbeing of business. So if we have not validated our DDoS protection, the result will be extended downtime. Proactive measures against DDoS and mitigation appliances are varying such as firewalls and routers. The

validation plan will not guarantee that the mitigation services will work as suggested. We suggest that we could avoid a heavy and costly down time if we tested our DDoS mitigation strategy before the attack hits. Validating and modifying mitigation strategy when need be. We recommend the following:

- Generate few gigabits of controlled traffic to validate the alerting features of the services.
- Test Small level of traffic without scrubbing and without any DDoS protection to validate that on premise monitoring are functioning correctly.
- Schedule validation tests on a regular basis yearly or quarterly to validate that the service is working properly.

Access control, in general cloud computing will typically comprise of several layers from physical up to visualization layer and potentially multiple application layers. The data type in the cloud ranging from important to highly sensitive one, all different types may reside in the cloud, and some are accessible with low privileges while other data require administrative privileges. The identity management, access authorization, and authentication mechanisms used by the cloud service must enforce appropriate protections and utilize government approved cryptographic mechanisms. Authentication mechanisms must be evaluated from standard functions to ensure compliance and safe handling and transmission of user credentials.

- Cloud services may provide a limited ability to audit the roles and permissions assigned to all accounts within the customer's portion of the cloud service.
- Audit record retention and availability may be limited with cloud services.
- Cloud service providers may be able to enforce particular password rules or lifespan.
- Deliver mandatory data encryption.

Malicious users, hackers who are always trying to achieve self-interest goals, Hackers and malicious code author can conduct different activities with relative impunity. As cloud service providers are targeted for their weak registration systems and limited fraud detection capabilities. For example some cybercriminals use rich content applications such as flash files that enable them to hide their malicious code and utilize users' browsers to install malware.

- Analyze data protection at both design and run time.
- Conduct vulnerability scanning and configuration audit
- Perform code scanning on a regular basis.
- Monitor unauthorized access.
- Enforce service level agreement for patching and vulnerability remediation.

VI. Overall assessment and monitoring: during the process, all involved teams were asked to monitor their works and provide a summary of their findings and progress. At the end, we found that the risk assessment meet the plan by 70%.

4.5 How to Benefit from Using Cloud Computing and Risk Management Framework

Major growth in cloud computing adoption can be predictable. Predictions for growth in the cloud services market range between $46.3 billion reported in 2008 to $148.8 billion and $150 billion by 2014 and $222.5 billion market by 2015 (Carroll & Kotzé, 2011). Cloud computing spending is predicted to grow from $16 billion in 2008 to around $55 billion in 2014. These predictions for growth are based on the realization of the many benefits of cloud computing. Cloud computing benefits are listed in Figure 7 arranged from the highest occurrence (therefore cited most in literature) to the lowest (Carroll & Kotzé, 2011). Cost efficiency is the main driver for cloud computing adoption. Other primary advantages include scalability, flexibility, agility, better IT resource management and business focus, efficiency, higher

reliability and availability, rapid development, deployment and change management, better performance and greater mobility. Improved automation, support and management, improved security, and green-IT data centers were also cited as valuable drivers for moving to the cloud (Carroll & Kotzé, 2011).

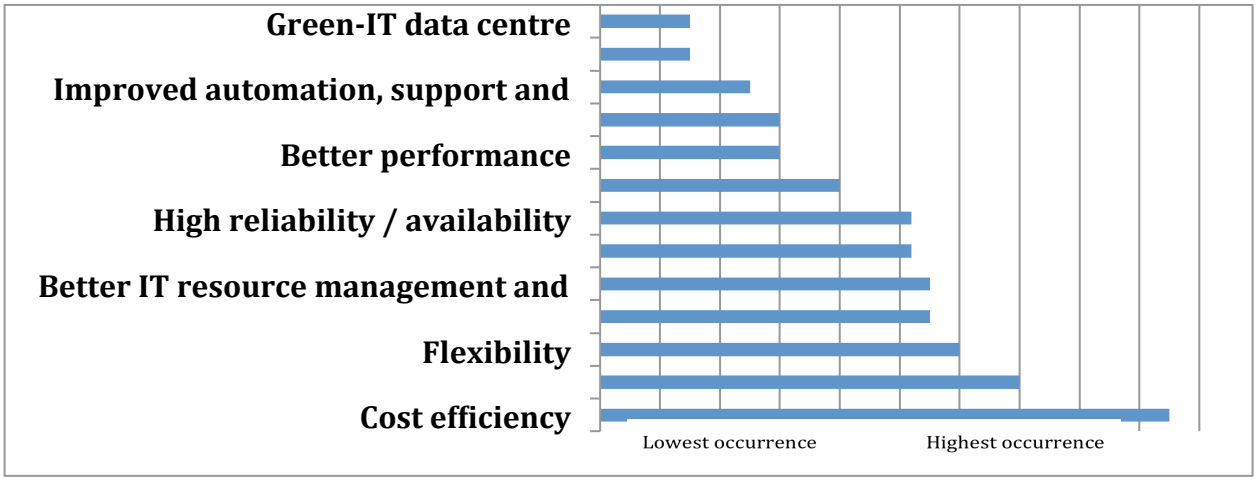

Figure 7: Cloud Computing Benefits

In this rapid era of technology and innovations, business is growing rapidly. The demands of customers are increasing with high speed and they need the products more quickly with less time. In order to achieve these demands, business organizations around the globe need to communicate and collaborate by using IT resources such as collaborative applications and remote access web services. Cloud computing provides these business demanded application on the cloud or internet. Users are able to access these applications at anytime and anywhere. Business people can arrange their meetings and share messages or emails by using cloud applications provided by various vendors. Cloud computing has moved mobility ahead in business, as well. Business people can access the services of cloud just by using a web browser on a Smartphone, tablet, or notebook. There is no need to use laptops or desktop computers. With the help of cloud applications, salespersons can view updated orders from customers at anytime. The quick processing of customer orders enables organizations to achieve customer

satisfaction levels that automatically lead to increased productivity and profit (Brohi & Bamiah, 2011).

A cloud computing approach to telecommunications services can offer many benefits, including cost reduction and service flexibility. By moving software and infrastructure to the provider's remote data center, customers can lower some of the upfront risks and difficulties associated with realizing the benefits of new technology. Customers may achieve a reduction in capital costs, including the upfront investment in new infrastructure, new software licenses, implementation services, and personnel hiring and/or training. In addition, less equipment means that less physical space at a customer site is needed to store such devices. Further, there is a lower costs as a result of reductions in planning, purchasing, installing, maintaining, managing, and supporting the software and infrastructure, as well as hiring, training, and managing an IT staff.

In addition, customers are attracted to the flexibility of being able to quickly set up and implement an IT solution, being able to access services from anywhere at any time via the Internet, and being able to quickly add and remove IT resources on demand, so that customers can effectively respond to internal business requirements and changing market conditions.

Cloud computing enables organizations to become more competitive due to flexible and active computing platforms, providing for scalability and high-performance resources and highly reliable and available applications and data.

Cloud computing is a flexible model and provides on-demand business scalability by using on-demand cloud services such as SaaS, PaaS or IaaS. Scalability is another aspect of cloud computing that can provide an advantage to business. Depending on service needs at any given time period, a company can scale back the amount of virtual server space they need, or

raise it according to their pattern of growth. This is especially useful for new businesses that are trying to save money at every possible turn. A smaller business does not have to pay a fixed rate for a certain amount of data center hosting that they might not even use. In this way, a company can scale up the level of space they need on a dedicated server through cloud computing. A low-cost dedicated server can easily save a business thirty to forty percent of their average annual cost for IT. If an organization is a SaaS user, it can request to adopt PaaS or IaaS whenever required. With an on-demand integration solution, companies can quickly and easily increase or decrease connections, transactions, or the number of companies in their integration community, and then scale up when business requires it (Brohi & Bamiah, 2011).

'Going green ' and saving costs are a key focus point for organizations. Cloud computing helps organizations to reduce power, cooling, storage and space usage and thereby facilitates more sustainable, environmentally responsible data centers (Carroll & Kotzé, 2011).

In case of disasters, an offsite backup is always helpful. Keeping crucial data backed up using cloud storage services is the need of the hour for most of the organizations. Also cloud storage services not only keep your data off site, but they also ensure that they have systems in place for disaster recovery (Jadeja & Modi. (2012).

Cloud computing makes it easier for enterprises to scale their services – which are increasingly reliant on accurate information –according to client demand. Since the computing resources are managed through software, they can be deployed very fast as new requirements arise. In fact, the goal of cloud computing is to scale resources up or down dynamically through software APIs depending on client load with minimal service provider interaction (Marston, Li, Bandyopadhyay, Zhang & Ghalsasi, 2011).

There are also some benefits of having such framework within a company. Risk

management can help with the planning and processing of newer technology that will allow for easier, quicker development times. Breaking down the process and planning of a project while using the risk management framework can increase the productivity of projects while also remaining cost effective in the developing of newer software.

Having a risk management framework will ensure that when the risk appear the company will know how to effectively handle the issue. Business priority is to keep the confidentiality of client's information as well as company's secret. Risk Management allows for planning or processing a control of attributes that would assist in allowing the business to expand to client while also providing no attention to the company's communication.

Louie (2014), the head of Trust, Safety, and Security at Dropbox, proved that cloud computing is secured and is not threatening as many people think. It is that no one — regardless of their resources — is 100% secure, but everyone strives to get as close as possible. It is all about how you manage those risks and benefit from this new technology.

It is significant to know how to evaluate whether those advantages are right for you as individual user and for you company or organization. These are some guidelines that can help:

I. Recognize your real needs: Understand what your data security and governance requirements are and should be. Establish realistic, grounded expectations around the level of security and control your need and want. Make sure you know what problems you are trying to solve. Do not ask for the Fort Knox of security systems if it is not what you really need, or you will end up spending more money, time, and resources than you should. Fort Knox is the premier home security installation and monitoring company offering consumers and businesses options from very cost-effective alarm monitoring to the most cutting-edge Home Automation systems giving users complete control of multiple features of their alarm systems.

II. Remember the user: Look beyond traditional security measures to usability and adoption. If you or your employees will not use the solution, there is no point in implementing it, no matter how secure it may appear to be. When employees start using workarounds that you have little control over, you will find that they pose a much bigger security risk.

III. Worry less about location: Keep an open mind. The security of your data is more important than its location. A distributed information storage infrastructure is secure by design, and certainly more so than keeping all your information unencrypted in a single location. Storing data remotely guarantees data redundancy, easy access no matter where you are, and scalability with no impact on performance and speed.

IV. Focus on access: Remember that controlling access is key. Look at how your data is accessed, and look specifically at holes that could be exploited. Most data breaks occur by finding vulnerabilities and poor end user practices, regardless of whether your information is cloud-based or on sites. Make sure that you and your employees are not making common mistakes like reusing passwords. Ensure that you have configured devices with appropriate encryption and set up a strong device management system.

V. Assure credibility: When evaluating a partner, check for certifications and compliance with recognized standards and frameworks, levels and types of encryption, and product features that give you control and visibility.

VI. Invest in a 24/7 approach: Finally, make sure your providers are auditing, monitoring, and testing security on a continuous basis.

CHAPTER 5

Conclusion and Future Work

5.1 Conclusion

In recent years, cloud computing has gained much popularity in the IT industry. Cloud computing is a computing resource with deployment and service models that enables users to get computing resources and applications from any locations via an Internet connection. The powerful characteristic of cloud computing is that no special devices or software are required to get the service. User only needs Internet and remote servers in order to use cloud computing services. Cloud computing brings us both opportunities and challenges. Reduced cost, speed of deployment, scalability, less requirements for operating IT functions and other environmental benefits, such as less physical space, are among the benefits cloud computing provides. However, a large number of organizations and users in general do not use or adopt this new technology mainly because of security concerns and low trust. To prevent serious problems occurring with security aspect of cloud computing, we provided a risk management framework that can be applied for this purpose. The main goals are to raise trust between providers and users and to increase the number of users and adopters of cloud computing. To accomplish this, this thesis has provided a comprehensive cloud computing risk management framework based on previous work. This Risk Management framework consisting of six stages namely (1) understand the business context, (2) identify the business technical risk, (3) synthesize and prioritize the risk, (4) define the risk mitigation strategy, (5) carry out required solutions and validate that they are resolved and (6) overall assessment and monitoring of the system is a novel idea for effectively monitoring, assessing and combating threats both from adversarial and non-adversarial sources. The first five steps are the well-known risk management stages but this

research has adopted a more robust approach to each of them. The sixth stage is a new stage that is unique to this work. This thesis highlights the details of these approaches used in the first five steps as well as the explanation of the sixth step.

To clarify these steps, a scenario explaining a step-by-step approach to applying this risk management framework to a hypothetical cloud computing provider has been outlined. The advantage of this Risk Management Framework lies in the fact that it can be used in wide range and flexibility because it can fit with small and large enterprise. Besides, the RMF is not specific to security risks; it can be applied in non-software situations.

5.2 Future Work

A more logical extension of this research work will be the actual application of the system to an existing system to evaluate the performance. Also, a good performance metric for evaluating the system can be designed. A comprehensive comparison of this approach to existing RMF's will also help highlight the strengths and the weaknesses of this approach.

In addition, searching for other reasons that decrease the trust and adaption of cloud computing technology can extend this work. Proposing other solutions and system may be a good way to increase the trust and adaption between the users and providers. Another way to extend this thesis is to provide cloud computing providers with tested proven solutions that can attract users, business and organizations to adapt their services.

References

Alabbadi, Mohssen M. (2011). Cloud computing for education and learning: Education and learning as a service (ELaaS). Paper presented at the Interactive Collaborative Learning (ICL), 2011 14th International Conference on.

Archer, Jerry, Boehme, Alan, Cullinane, Dave, Kurtz, Paul, Puhlmann, Nils, & Reavis, Jim. (2010). Top threats to cloud computing v1. 0. Cloud Security Alliance.

Armbrust, et.al (2010). A view of cloud computing. Communications of the ACM, 53 (4), p. 50-58.

Arnold, Uwe, Oberlander, Jan, & Schwarzbach, Bjorn. (2013). Advancements in cloud computing for logistics. Paper presented at the Computer Science and Information Systems (FedCSIS), 2013 Federated Conference on.

Azimi-Sadjadi, M. R., & Zekavat, S. A. (2000, 2000). Cloud classification using support vector machines.

B. Karabacaka and I. Sogukpinarb, "A quantitative method for ISO 17799 gap analysis," Computers & Security, vol. 25, no. 6, pp. 413– 419, Sep 2006.

B. R. Kandukuri, V, R. Paturi and A. Rakshit, "Cloud security issues," in Proceedings of the 2009 IEEE International Conference on Services Computing, pp. 517-520, September 2009.

Benlian, Alexander, & Hess, Thomas. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. Decision Support Systems, 52(1), 232-246. doi: 10.1016/j.dss.2011.07.007

Bento, AL, & Bento, REGINA. (2011). Cloud Computing: A New Phase in Information Technology Management. Journal of Information Technology Management, 22(1), 39-

46.

Brender, Nathalie, & Markov, Iliya. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. International Journal of Information Management, 33(5), 726-733. doi: 10.1016/j.ijinfomgt.2013.05.004

Brohi, Sarfraz Nawaz, & Bamiah, Mervat Adib. (2011). Challenges and benefits for adopting the paradigm of cloud computing. International Journal of Advanced Engineering Sciences and Technologies, 2, 286-290.

Carroll, M., & Kotzé, P. (2011). Secure cloud computing: Benefits, risks and controls. IEEE.

Carroll, Mariana, Van der Merwe, A, & Kotze, P. (2011). Secure cloud computing: Benefits, risks and controls. Paper presented at the Information Security South Africa (ISSA), 2011.

Cha, S., Juo, P., Liu, L., & Chen, W. (2008). RiskPatrol: A risk management system considering the integration risk management with business continuity process. IEEE.

Cha, Shi-Cho, Juo, Pei-Wen, Liu, Li-Ting, & Chen, Wei-Ning. (2008). Riskpatrol: A risk management system considering the integration risk management with business continuity processes. Paper presented at the Intelligence and Security Informatics, 2008. ISI 2008. IEEE International Conference on.

Chonka, Ashley, Xiang, Yang, Zhou, Wanlei, & Bonti, Alessio. (2011). Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications, 34(4), 1097-1107. doi: 10.1016/j.jnca.2010.06.004

Claycomb, William R, & Nicoll, Alex. (2012). Insider threats to cloud computing: Directions for new research challenges. Paper presented at the Computer Software and Applications Conference (COMPSAC), 2012 IEEE 36th Annual.

Cloud Security Alliance. (2010). Top threats to cloud computing V1.0. https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Dasgupta, Partha, LeBlanc, Richard J., Ahamad, Mustaque, & Ramachandran, Umakishore. (1991). The Clouds distributed operating system. IEEE Computer, 24(11), 34-44.

Dou El Kefel, Mansouri, & Mohamed, Benyettou. (2013). Risk management in cloud computing. Paper presented at the Innovative Computing Technology (INTECH), 2013 Third International Conference on.

Dwight, Herbert Bristol. (1930). Calculation of protection of a transmission line by ground conductors. AIEE, Journal of the, 49(5), 354-357.

Ernawati, T, & Nugroho, DR. (2012). IT risk management framework based on ISO 31000: 2009. Paper presented at the System Engineering and Technology (ICSET), 2012 International Conference on.

Etro, Federico. (2009). The economic impact of cloud computing on business creation, employment and output in Europe. Review of Business and Economics, 54(2), 179-208.

Feizi, Soheil, Zhang, Amy, & Médard, Muriel. A Network Flow Approach in Cloud Computing.

Fitó, Josep Oriol, Macías Lloret, Mario, & Guitart Fernández, Jordi. (2012). Toward business-driven risk management for cloud computing.

Gang, Chen. (2009). Mathematics and Applications of Risk Management in E-commerce. Paper presented at the Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on.

Glaser, J. (2011). Cloud computing can simplify HIT infrastructure management. Healthcare financial management: journal of the Healthcare Financial Management Association, 65(8), 52-55.

Green, Matthew. (2013). The threat in the cloud. Security & Privacy, IEEE, 11(1), 86-89.

Gupta, Prashant, Seetharaman, A., & Raj, John Rudolph. (2013). The usage and adoption of cloud computing by small and medium businesses. International Journal of Information Management, 33(5), 861-874. doi: 10.1016/j.ijinfomgt.2013.07.001

Han, Y. (2011). Cloud Computing: Case Studies and Total Costs of Ownership. Information Technology and Libraries, 30 (4).

Hutchings, A., Smith, R., & James, L. (2013). Cloud computing for small business: Criminal and security threats and prevention measures. Australian Institute of Criminology.

Hwang, J., Chuang, H., Hsu, Y., & Wu, C. (2011). A business model for cloud computing based on a separate encryption and decryption service. IEEE.

Hwang, Jing-Jang, Chuang, Hung-Kai, Hsu, Yi-Chang, & Wu, Chien-Hsing. (2011). A business model for cloud computing based on a separate encryption and decryption service. Paper presented at the Information Science and Applications (ICISA), 2011 International Conference on.

Initiative, Joint Task Force Transformation. (2011). SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View.

Jadeja, Yashpalsinh, & Modi, Kirit. (2012). Cloud computing-concepts, architecture and challenges. Paper presented at the Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on.

Khalil, Issa M., Khreishah, Abdallah, Bouktif, Salah, & Ahmad, Azeem. (2013, 2013/04//). Security Concerns in Cloud Computing.

Khan, Afnan Ullah, Oriol, Manuel, Kiran, Mariam, Jiang, Ming, & Djemame, Karim. (2012, 2012). Security risks and their management in cloud computing.

Kudtarkar, P., Deluca, T. F., Fusaro, V. A., Tonellato, P. J., & Wall, D. P. (2010). Cost-effective cloud computing: a case study using the comparative genomics tool, roundup. Evol Bioinform Online, 6, 197-203. doi: 10.4137/EBO.S6259

Lenk, Alexander, Klems, Markus, Nimis, Jens, Tai, Stefan, & Sandholm, Thomas. (2009). What's inside the Cloud? An architectural map of the Cloud landscape. Paper presented at the Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing.

Lhannaoui, Hanane, Kabbaj, Mohammed Issam, & Bakkoury, Zohra. (2013). Towards an approach to improve business process models using risk management techniques. Paper presented at the Intelligent Systems: Theories and Applications (SITA), 2013 8th International Conference on.

Liu, Wentao. (2012). Research on cloud computing security problem and strategy. Paper presented at the Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on.

Lonea, A., Popescu, D., & Tianfield, H,.2013 Detecting DDoS Attacks in Cloud Computing Environment . INT J COMPUT COMMUN

Louie, Cory. (2014). The truth about cloud security.

Loyola, DGR. (2004). Automatic cloud analysis from polar-orbiting satellites using neural network and data fusion techniques. Paper presented at the Geoscience and Remote Sensing Symposium, 2004. IGARSS'04. Proceedings. 2004 IEEE International.

Marston, Sean, Li, Zhi, Bandyopadhyay, Subhajyoti, Zhang, Juheng, & Ghalsasi, Anand. (2011). Cloud computing — The business perspective. Decision Support Systems, 51(1), 176-189. doi: 10.1016/j.dss.2010.12.006

McGraw, G. (2006). Software security: Building security in. Pearson Education, Inc.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. U.S.Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory. Retrieved on February 16, 2014 from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Moyo, Moses, Abdullah, Hanifa, & Nienaber, Rita C. (2013). Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems. Paper presented at the Information Security for South Africa, 2013.

Perera, Jeevan, & Holsomback, Jerry. (2005, 2005). An integrated risk management tool and process.

Qaisar, S., & Khawaja, K. (2012). Cloud computing: Network/security threats and countermeasures. Interdisciplinary Journal of Contemporary Research in Business, 3 (9), p. 1323-1329.

Rimal, BP,. Jukan, A,. Katsaros. D,. & Goeleven Y. (2011). Architectural requirements for cloud computing systems: An enterprise cloud approach. Journal of Grid Computing, 9(1), p. 3–26.

Roy, Geoffrey G. (2004). A risk management framework for software engineering practice. Paper presented at the Software Engineering Conference, 2004. Proceedings. 2004 Australian.

Ryan, Mark D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. Journal of Systems and Software, 86(9), 2263-2268. doi: 10.1016/j.jss.2012.12.025

S. Tanimoto, M. Hiramoto, M. Iwashita, etc. Risk management on the security problem in cloud computing. In Proc. Of ACIS/JNU international conference on computers, networks, systems, and industrial engineering, 2011.

Sadiku, M., Musa, S., & Momoh, O. (2014). Cloud computing: Opportunities and challenges. IEEE, 33 (1), p. 34-36.

Salah, Khaled, Calero, Jose M. Alcaraz, Zeadally, Sherali, Al-Mulla, Sameera, & Alzaabi, Mohammed. (2013). Using cloud computing to implement a security overlay network. IEEE Security & Privacy, 44-53.

Samejima, Masaki, & Yajima, Hiroshi. (2012). IT risk management framework for business continuity by change analysis of information system. Paper presented at the Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on.

Schoenthaler, Frank. (2002). Risk management in challenging business software projects. Paper presented at the Requirements Engineering, 2002. Proceedings. IEEE Joint International Conference on.

Shaikh, Farhan Bashir, & Haider, Sajjad. (2011). Security threats in cloud computing. Paper presented at the Internet technology and secured transactions (ICITST), 2011 international conference for.

Special Publication 800-30. Information Secuirty: Guide for Conducting Risk Assessments. America. National Institute of Standards and Technology, 2011.

Stoneburner, G,. Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technology. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930

Tan & Ai. (2011). The issues of cloud computing security in high-speed railway. International Conference on Electronic & Mechanical Engineering and Information Technology, 8, p. 4358 – 4363.

Tan, WenAn, Sun, Yong, Li, Ling Xia, Lu, GuangZhen, & Wang, Tong. (2013). A Trust Service-Oriented Scheduling Model for Workflow Applications in Cloud Computing. IEEE Systems Journal, 1-11. doi: 10.1109/JSYST.2013.2260072

Tan, Xiang, & Ai, Bo. (2011). The issues of cloud computing security in high-speed railway. Paper presented at the Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on.

Tanimoto, Shigeaki, Hiramoto, Manami, Iwashita, Motoi, Sato, Hiroyuki, & Kanai, Atsushi. (2011, 2011/05//). Risk Management on the Security Problem in Cloud Computing.

Tracey, James H., Pottinger, Hardy J., & Rechtien, R. D. (1975). A computer-automated laboratory system in a university environment. Proceedings of the IEEE, 63(10), 1486-1495.

Uchida, Noriki, Takahata, Kazuo, & Shibata, Yoshitaka. (2011, 2011/10//). Proposal of Overlay Cloud Computing System by Virtual Autonomous Network Configuration.

Wall, Dennis, Parul, Kudtarkar, Todd, F. DeLuca, Vincent, A. Fusaro, & Peter, J. Tonellato. (2010). Cost-Effective Cloud Computing: A Case Study Using the Comparative Genomics Tool, Roundup. Evolutionary Bioinformatics. doi: 10.4137/EBO.S6259

Wang, H. (2011). Cloud computing-based IT solutions for organizations with multiregional branch offices. Academic Conference Limited. Toronto: Canada. P. 435-440.

Wang, X., Wang, b., & Huang, j. (2011). Cloud computing and its key techniques. Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference

IEEE, 2, p. 404 – 410.

Xia, Li. (2012, 2012/10//). Issue about Security of E-business Under the Pattern of Cloud Computing.

Xiao, Zhifeng, & Xiao, Yang. (2013). Security and privacy in cloud computing. Communications Surveys & Tutorials, IEEE, 15(2), 843-859.

Xie, Feng, Peng, Yong, Zhao, Wei, Chen, Dongqing, Wang, Xiaoran, & Huo, Xingmei. (2012, 2012). A risk management framework for cloud computing.

Xin, Zhang, Song-qing, Lai, & Nai-wen, Liu. (2012). Research on cloud computing data security model based on multi-dimension. Paper presented at the Information Technology in Medicine and Education (ITME), 2012 International Symposium on.

Xiong, Fenghua, & Sun, Weidong. (1993, 1993). A study on cloud clearing method for satellite images based on isotherm's auto-connection.

Xu, Xun. (2012). From cloud computing to cloud manufacturing. Robotics and Computer-Integrated Manufacturing, 28(1), 75-86. doi: 10.1016/j.rcim.2011.07.002

Zhang, Xuan, Wuwong, Nattapong, Li, Hao, & Zhang, Xuejie. (2010, 2010/06//). Information Security Risk Management Framework for the Cloud Computing Environments. on Computer and Information Technology.

Zhu, Jinzy. (2010). Cloud Computing Technologies and Applications. 21-45. doi: 10.1007/978-1-4419-6524-0_2

Appendix

1. Distributed Denial of Service (DDoS) attack on cloud computing.

DDoS Attack on cloud computing are launched with the intention to have a negative impact in the availability of the targeted application, data or services. Protecting and ensuring availability against DDoS can be challenging. For maintaining availability by many service providers and data centers operator with a good track record of availability by properly assessing the risk to availability posed by the cloud. Successful DDoS have negative impacts on the business goals of the cloud computing. Nevertheless, the reputational damage will be listed as another negative impact as customers will no longer have confidence in the service we provide. The mitigation steps against such sever attack is by understanding the infrastructure of the cloud: avoid single point of failure. Private clouds might reduce the availability risk but add more cost. The analyses team can balance the risk by using multiple data centers with the risk of a single suite failure. Their first promise was to deliver the service during the year with no interruption; they recommended that the following are the best practices for DDoS mitigation service and validation.

- With the DDoS mitigation service active, verify that all applications are performing properly.
- Verifying that all routing to DNS is working.
- Conduct baseline testing and calibrate system to remove any vulnerability in the network.
- Schedule validation test on regular basis with DDoS mitigation service to validate that the service configuration is still working correctly.
- If network issues arise during testing, then we need to make modifications, such as modified firewall rules, firmware updates or router reconfigurations.

2. Security weaknesses cause service and storage failures.

CloudPro offers and provides users/organizations with various types of services including unlimited bandwidth and storage capacity. As they are trying to generate more revenues and try to make a solid company and be one of the renounce cloud provider in the market, they did offer free limited trials periods but unfortunately that would give the hacker access to their cloud immorally, the impact may include but not limited to decoding and cracking of passwords, launching potential attack points and executing malicious codes. Hackers and malicious code author can conduct different activities with relative impunity. As cloud service providers are targeted for their weak registration systems and limited fraud detection capabilities. For example some cybercriminals use rich content applications such as flash files that enable them to hide their malicious code and utilize users' browsers to install malware. The Impact caused by this type of attacks can harm the business. They expect a huge financial loss, damage to the company reputation, and violate data privacy and critical information and data leakage. To reduce the potential damage:

- They don't keep all the files in one place; we split them over different data centers.
- They obfuscate our data, not simple encryption.
- File names are randomized so as to not match content type to owner. Even if you know what you are seeking for it would be hard to find.

3. Identity and access control are failed to control threats and vulnerabilities during communication sessions.

One of the most important security mechanisms used to protect other people personal data and prevent unauthorized access is access control. It provides a flexible approach that allows data owners to integrate data access polices with encrypted data. In order to protect the customer sensitive data from misuse we support an efficient access control mechanisms for the cloud services with the help of cryptographic integer comparisons and proxy-based re-encryption mechanism in the current time. They prove the security effectiveness of our scheme. The major impact it has is damage to the company reputation as this would be interpreted as weak architectural design and consequently will cause a huge financial loss.

- Keep tracking of users' activity.
- Mapping users and their privileges.
- Access control that will bundle the user identity with the requested service.