



SCHOOL OF ECONOMICS AND MANAGEMENT

Lund University

“CLOUD COMPUTING’S EFFECT ON ENTERPRISES”

“...in terms of Cost and Security”

Master’s Thesis, 15ECTS

Supervisor: Mr. Odd Steen

Submitted: January, 2011

Author: Rehan Saleem (831015-T132)

LUND UNIVERSITY

Informatics

“CLOUD COMPUTING’S EFFECT ON ENTERPRISES”

“...in terms of Cost and Security”

Master Thesis submitted January, 2011

Size: 89 Pages

Supervisor: Odd Steen.

Examiners: Björn Johansson, Paul Pierce.

Abstract

Innovations are necessary to ride the inevitable tide of change. Most of enterprises are striving to reduce their computing cost through the means of virtualization. This demand of reducing the computing cost has led to the innovation of Cloud Computing. Cloud Computing offers better computing through improved utilization and reduced administration and infrastructure costs. Cloud Computing is the sum of Software as a Service (SaaS) and Utility Computing.

Cloud Computing is still at its infant stage and a very new technology for the enterprises. Therefore, most of the enterprises are not very confident to adopt it. This research paper tackles this issue for enterprises in terms of cost and security. In this paper I discuss the benefits and drawbacks an enterprise can have while they adopt Cloud Computing in terms of Cost and Security.

In the end, concluding that Cloud Computing is better for medium and small sized enterprises as compared to large enterprises in terms of both cost and data security.

Key words:

Cloud Computing, SaaS, IaaS, PaaS, Elasticity, Cost, Security

TABLE OF CONTENTS

1. INTRODUCTION AND BACKGROUND	4
1.1 RESEARCH QUESTION	6
1.2 PURPOSE OF RESEARCH	6
1.3 RESEARCH DELIMITATION	6
2. THEORITICAL BASELINES.....	8
2.1 CLOUD COMPUTING	8
2.1.1 DEFINITION	8
2.1.2 CLOUD COMPUTING ARCHITECTURE.....	9
2.1.3 CLOUD COMPUTING EVOLUTION	11
2.1.4. CLOUD COMPUTING ADOPTION	14
2.2 CLOUD COMPUTING AND COST	15
2.2.1 COST IN CONSUMER PERSPECTIVE	16
2.2.2 COST IN PROVIDER'S PERSPECTIVE.....	17
2.2.3 CLOUD COMPUTING'S COST EFFECT	18
2.2.3.1 BENEFITS	18
2.2.3.2 DRAWBACKS	20
2.2.4 CLOUD COMPUTING VERSUS DESKTOP GRID.....	20
2.3 CLOUD COMPUTING AND DATA SECURITY	21
2.3.1 DATA SECURITY IN CLOUD.....	22
2.3.2 SECURITY BENEFITS OF CLOUD COMPUTING.....	27
2.4 SUMMARY	34
3. RESEARCH STRATEGY	37
3.1 METHOD SELECTION	37
3.2 DATA ANALYSIS	41
3.3 RESEARCH QUALITY	44
4. EMPIRICAL STUDY	46
4.1 INTERVIEWS	46
4.1.1 CLOUD COMPUTING AND COST.....	46
4.1.2 CLOUD COMPUTING AND DATA SECURITY.....	49
4.1.3 CLOUD COMPUTING AND PROVIDER'S PERSPECTIVE	52
4.2 INTERVIEWS DISCUSSION	56
4.2.1 THE COST EFFECT.....	59
4.2.2 THE SECURITY EFFECT	62
5. CONCLUSION.....	69
APPENDIX A: INTERVIEW 1.....	71
APPENDIX B: INTERVIEW 2.....	76
APPENDIX C: INTERVIEW 3.....	80
REFERENCES	86

1. INTRODUCTION AND BACKGROUND

Cloud Computing has become one of the most talked about technologies in recent times and has got lots of attention from media as well as analysts because of the opportunities it is offering. The market research and analysis firm IDC suggests that the market for Cloud Computing services was \$16billion in 2008 and will rise to \$42billion/year by 2012 (Gleeson, 2009). It has been estimated that the cost advantages of Cloud Computing to be three to five times for business applications and more than five times for consumer applications (Lynch, 2008). According to a Gartner press release from June 2008, Cloud Computing will be “no less influential than e-business” (Gartner, 2008).

Enterprises have been striving to reduce computing costs and for that reason most of them start consolidating their IT operations and later using virtualization technologies. For the good of the enterprises there is a new technology to help them in this i.e. Cloud Computing. Cloud Computing claims to take enterprises search to a new level and allows them to further reduce costs through improved utilization, reduced administration and infrastructure cost and faster deployment cycles (Boss et al., 2007, p2).

Cloud Computing is a term used to describe both a platform and type of application. As a platform it supplies, configures and reconfigures servers, while the servers can be physical machines or virtual machines. On the other hand, Cloud Computing describes applications that are extended to be accessible through the internet and for this purpose large data centers and powerful servers are used to host the web applications and web services (Boss et al., 2007, p2).

The cloud is a metaphor for the Internet and is an abstraction for the complex infrastructure it conceals. There are some important points in the definition to be discussed regarding Cloud Computing. Cloud Computing differs from traditional computing paradigms as it is scalable, can be encapsulated as an abstract entity which provides different level of services to the clients, driven by economies of scale and the services are dynamically configurable (Foster et al., 2008, p1).

There are many benefits stated of Cloud Computed by different researchers which make it more preferable to be adopted by enterprises. Cloud Computing infrastructure allows enterprises to achieve more efficient use of their IT hardware and software investments. This is achieved by breaking down the physical barrier inherent in isolated systems, automating the management of the group of the systems as a single entity. Cloud Computing can also be described as ultimately virtualized system and a natural evolution for data centers which offer automated systems management (Boss et al., 2007, p4).

Enterprises need to consider the benefits, drawbacks and the effects of Cloud Computing on their organizations and usage practices, to make decision about the adoption and use. In the enterprise, the “adoption of Cloud Computing is as much dependent on the maturity of organizational and cultural (including legislative) processes as the technology, per se” (Fellowes, 2008).

Many companies have invested in Cloud Computing technology by building their public clouds, which include Amazon, Google and Microsoft. These companies are often releasing new features and updates of their services. For instance Amazon Web Services (AWS) released a Security² and Economics³ center on their website to have academic and community advice regarding these issues (Khajeh-Hosseini et al., 2010b, p2). This shows that there are still lots of doubts about the costs and security for enterprises to adopt Cloud Computing. Hence, the issues of economics and security in Cloud Computing for enterprises must be researched.

As large organizations are inherently complex hence, it is very important for Cloud Computing to deliver the real value rather than just be a platform for simple tasks such as application testing or running product demos. For this reason, issues around migrating application systems to the cloud and satisfying the needs of key stakeholders should be explored. The stakeholders include technical, project, operations and financial managers as well as the engineers who are going to be developing and supporting the individual systems. For enterprises economics or cost factor is important but at the same time

customer relationships, public image, flexibility, business continuity and compliance are of same importance (Khajeh-Hosseini et al., 2010b, p2). Hence, enterprises need to understand how Cloud Computing affects all these however; I shall discuss the following specific issues in this paper.

- The economic and organizational implications of the cost model in Cloud Computing.
- The data security, availability and privacy issues that Cloud Computing raises.

1.1 RESEARCH QUESTION

As Cloud Computing is one of the most talked about technologies now days and it has great importance in enterprises because of the cost and computational promises it offers. I will conduct the research on the issue of Cloud Computing and Enterprises. Fox Mobile Group is an enterprise which is using Cloud Computing and I will study them to answer my research question which is:

What are the perceived benefits and drawback regarding cost and data security for Enterprises to adopt Cloud Computing?

1.2 PURPOSE OF RESEARCH

The purpose of the thesis is to find out the benefits and drawbacks in regards with cost, data security and data availability; enterprise can have by the use of Cloud Computing for the implementation and management of their information system. Finally concluding the factors in terms of cost and data security, enterprises should keep in mind while adopting Cloud Computing for the effective and efficient use of their information system.

1.3 RESEARCH DELIMITATION

During my research I will not consider the SaaS (Software as a Service) and PaaS (Platform as a Service) of Cloud Computing as the enterprise which I am focusing i.e.

Cloud Computing effect on Enterprises

Fox Mobile Group is not using it. I will not study the whole information system of the enterprises but will focus on few divisions or parts of the information system (the divisions will be chosen after first interview with the company) in which enterprises are using Cloud Computing technology. I will also not discuss the Legal issues in the security of Cloud Computing.

2. THEORITICAL BASELINES

The aim of this part is to introduce the theoretical framework of my research work.

2.1 CLOUD COMPUTING

2.1.1 DEFINITION

There have been many definitions of Cloud Computing by different researchers. Barkley RAD defines Cloud Computing as:

“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. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud; the service being sold is Utility Computing. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public. Thus, Cloud Computing is the sum of SaaS and Utility Computing, but does not include Private Clouds. People can be users or providers of SaaS, or users or providers of Utility Computing.” (Armbrust et al., 2009, p6)

The summary of the features of Cloud Computing described by Stanoevska-Slabeva and Wozniak is (Stanoevska-Slabeva and Wozniak, 2009, p50):

- Cloud Computing is a new computing paradigm.
- Infrastructure resources (hardware, storage and system software) and applications are provided in X-as-a-Service manner. When these services are offered by an independent provider or to external customers, Cloud Computing is based on pay-per-use business models.
- Main features of Clouds are virtualization and dynamic scalability on demand.

- Utility computing and SaaS are provided in an integrated manner, even though utility computing might be consumed separately.
- Cloud services are consumed either via Web browser or via a defined API.

2.1.2 CLOUD COMPUTING ARCHITECTURE

NIST (National Institute of Standards and Technology) is a well accepted institution all over the world for their work in the field of Information Technology. I shall present the working definition provided by NIST of Cloud Computing. NIST defines the Cloud Computing architecture by describing five essential characteristics, three cloud services models and four cloud deployment models (Cloud Security Alliance, 2009, p14).

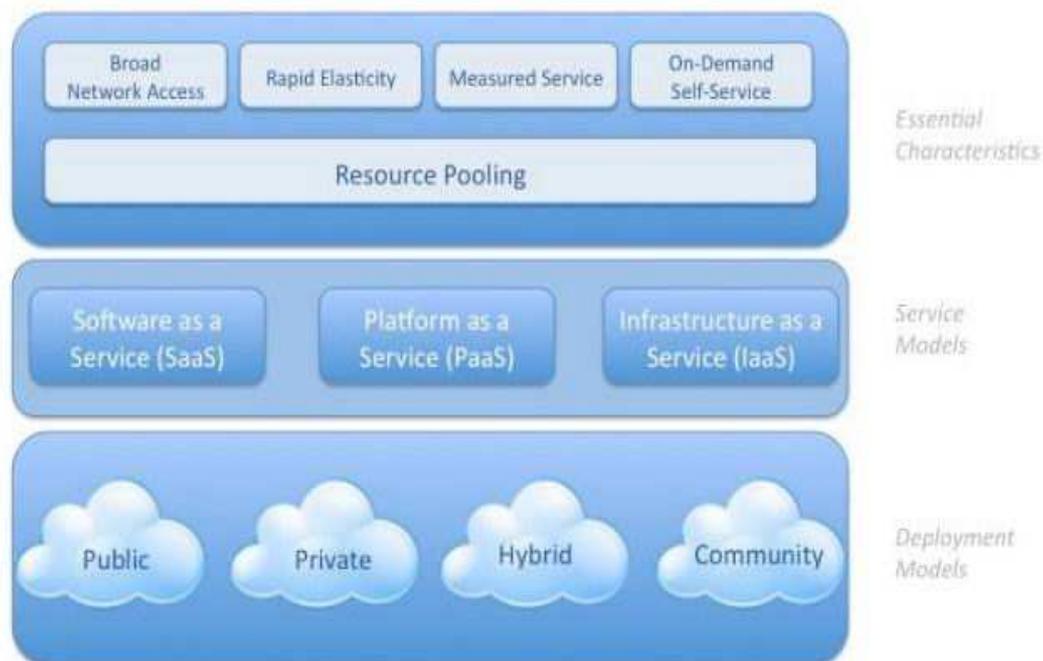


Figure 1 - Visual model of NIST Working Definition of Cloud Computing (Cloud Security Alliance, 2009, p14)

Essential Characteristics of Cloud Computing

As described above, there are 5 essential characteristics of Cloud Computing which explains their relation and difference from traditional computing.

- *On-demand-self-service*
Consumer can provision or un-provision the services when needed, without the human interaction with the service provider.
- *Broad Network Access*
It has capabilities over the network and accessed through standard mechanism.
- *Resource Pooling*
The computing resources of the provider are pooled to serve multiple consumers which are using a multi-tenant model, with various physical and virtual resources dynamically assigned, depending on consumer demand.
- *Rapid Elasticity*
Services can be rapidly and elastically provisioned.
- *Measured Service*
Cloud Computing systems automatically control and optimize resource usage by providing a metering capability to the type of services (e.g. storage, processing, bandwidth, or active user accounts) (Cloud Security Alliance, 2009, p15).

Cloud Service Models

There are 3 Cloud Services Models and these 3 fundamental classifications are often referred to as “SPI model” i.e. software, platform or infrastructure as a service.

- *Cloud Software as Service*
This is a capability in which the consumer can use the provider’s applications running on the cloud.
- *Cloud Platform as Service*

In this type of service, the consumer can deploy, the consumer created or acquired applications created by using programming languages or tools provided by provider, on the cloud infrastructure.

- *Cloud Infrastructure as Service*

This is a capability provided to the consumer by which, it can provision processing, storage, networks and other fundamental computing resources where the consumers can deploy and run the software (i.e. operating systems, applications) (Cloud Security Alliance, 2009, p16).

Cloud Deployment Models

- *Public Cloud*

The cloud infrastructure is available to the general public.

- *Private Cloud*

The type of the cloud, that is available solely for a single organization.

- *Community Cloud*

In this type of cloud deployment model, the infrastructure of the cloud is shared by several organizations and supports a specific community with shared concerns.

- *Hybrid Cloud*

This is a cloud infrastructure that is a composition of two or more clouds i.e. private, community or public (Cloud Security Alliance, 2009, p17).

2.1.3 CLOUD COMPUTING EVOLUTION

There has always been a debate about the evolution of Cloud Computing and the most important point in that is Grid Computing. Some people call Cloud Computing and Grid Computing the same phenomena while others call Cloud Computing an extension of Grid computing. To find the truth we need to know about the Grid computing (Stanoevska-Slabeva, Wozniak, 2009, p59).

Grid Computing is a complex phenomenon which has evolved through earlier developments in parallel, distributed and HPC (High Performance Computing)

(Weishäupl et al., 2005 and Harms et al. 2006). One of the most cited definitions of Grid computing at the start was from Foster and Kesselman (1998).

“A computational grid is a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities.” (Stanoevska-Slabeva and Wozniak, 2009, p23)

After that, the development of support for generic IT resource sharing, started to be measured as the real Grid problem. According to Foster,

“The real and specific problem that underlies the Grid concept is coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations. The sharing that we are concerned with is not primarily file exchange but rather direct access to computers, software, data, and other resources, as is required by a range of collaborative problem-solving and resource brokering strategies emerging in industry, science, and engineering.” (Foster et al., 2001, p2)

Virtual organizations in this definition can be defined as the dynamic group of individuals, groups, or organization who define the conditions and rules for sharing resources (Joseph et al., 2004).

Some of the organizations have also defined the Grid computing with respect to the features. According to IBM

“Grid computing allows you to unite pools of servers, storage systems, and networks into a single large system so you can deliver the power of multiple-systems resources to a single user point for a specific purpose. To a user, data file, or an application, the system appears to be a single enormous virtual computing system.” (Kourpas, 2006, p13)

The description of Cloud Computing earlier and of Grid computing here shows that Cloud Computing and grid computing have many similarities. This leads to discussion

about the differences in these two technologies. The table below shows the technical differences among Cloud Computing and Grid computing presented by Katarina Stanoevska-Slabeva and Thomas Wozniak (Stanoevska-Slabeva and Wozniak, 2009, p59).

Table 1 – Grid and Cloud Computing Technically Compared (Stanoevska-Slabeva and Wozniak, 2009, p59)

	Grid Computing	Cloud Computing
Means of utilization (e.g. Harris 2008)	Allocation of multiple servers onto a single task or job	Virtualization of servers; one server to compute several tasks concurrently
Typical usage pattern (e.g. EGEE 2008)	Typically used for job execution, i.e. the execution of a program for a limited time	More frequently used to support long-running services
Level of abstraction (e.g. Jha et al. 2008)	Expose high level of detail	Provide higher-level abstractions

As presented in the table what makes Cloud Computing different from Grid computing is “virtualization”. Cloud Computing leverages virtualization to maximize the computing power. Virtualization, by separating the logical from the physical, resolves some of the challenges faced by grid computing” (Lynch, 2008). While Grid computing achieves high utilization by the allocation of multiple servers onto a single task or job, the virtualization of servers in Cloud Computing achieves high utilization by allowing one server to compute several tasks concurrently (Harris, 2008).

Along with the differences in technology among Grid computing and Cloud Computing, usage patterns are also different between them. Grid is usually used for job execution while clouds are more frequently used to support long-running services (EGEE, 2008, p4).

As mentioned above, there is a debate in the technology world that Cloud Computing has evolved from Grid Computing and that Grid Computing is the foundation for Cloud Computing. Foster et al. (2008) for example describe the relationship between Grid and Cloud Computing as follows:

“We argue that Cloud Computing not only overlaps with Grid Computing, it is indeed evolved out of Grid Computing and relies on Grid Computing as its backbone and infrastructure support. The evolution has been a result of a shift in focus from an infrastructure that delivers storage and compute resources (such is the case in Grids) to one that is economy based aiming to deliver more abstract resources and services (such is the case in Clouds).” (Foster et al., 2008, p2).

Thus we can summarize that Grid Computing is the starting point and basis for Cloud Computing. Cloud Computing essentially represents the increasing trend towards the external deployment of IT resources, such as computational power, storage or business applications, and obtaining them as services (Stanoevska-Slabeva and Wozniak, 2009, p61).

2.1.4. CLOUD COMPUTING ADOPTION

Cloud Computing is also about how IT is provisioned and used and not only about technological improvements of data centers (Creeger, 2009, p50). Enterprises must consider the benefits, drawbacks and other effects of Cloud Computing on their enterprises and usage practices before adopting and using Cloud Computing (Khajeh-Hosseini et al., 2010b, p2). In enterprises, the adoption of Cloud Computing is much dependent on the maturity of organizational and cultural processes as the technology per se (Fellowes, 2008). Some predict that adoption of Cloud Computing is not going to happen overnight, rather it could take 10 to 15 years before typical enterprise make this

shift (Sullivan, 2009, p1). Hence, we are currently at the start of a transition period during which many decisions need to be made with respect to adoption of Cloud Computing in the enterprise.

The decision to adopt Cloud Computing is challenging because of the range of practical and socio political reasons. It is not possible that all enterprises outsource their whole back end computing requirements to cloud providers rather; they will establish a heterogeneous computing environment which is based on dedicated servers, organizational clouds and possibly more than one public cloud provider. How the adoption to Cloud Computing is managed does not only depend on technical issues but also on socio-technical factors (i.e. cost, confidentiality and control), the impact on work practices and constraints derived from existing business models. Hence, the challenges that enterprises must address before Cloud Computing adoption are : i) to provide accurate information on costs of cloud adoption; ii) to support risk management; and iii) to ensure that decision makers can make informed trade-offs between the benefits and risks (Khajeh-Hosseini et al., 2010c, p4).

2.2 CLOUD COMPUTING AND COST

The economic appeal of Cloud Computing is often mentioned as “converting capital expenses to operating expenses” (Armbrust et al., 2009, p12). Enterprises using Cloud Computing pay differently depending on the agreement between them and the Cloud Computing providers. Usually Cloud Computing providers have detailed costing models which are used to bill users on *pay per use basis* (Khajeh-Hosseini et al., 2010b, p4). There are different cost models available in the market for Cloud Computing. However, the most used model is discussed by Armbrust, which is a short term billing model. Armbrust describes the short term billing model as one of the most interesting and novel feature of Cloud Computing.

Researchers have discussed the economics of Cloud Computing in two respects i.e. Consumer Perspective and Provider Perspective. Both the perspectives have different cost/price models.

2.2.1 COST IN CONSUMER PERSPECTIVE

In Consumer perspective I discuss the cost models which are adopted by providers for consumers to pay. Hence, in this view we see the pricing models from consumer point of view.

According to Armbrust (2009) Cloud Computing provide a costing model i.e. pay for use of computing resources on a short term basis when required and also release them when not required. Hence, by this way you let machines and storage go when they are no longer useful (Armbrust et al., 2009, p3).

For instance, Elastic Compute Cloud (EC2) from Amazon Web Services (AWS) is selling 1.0-GHz x86 ISA "slices" for 10 cents per hour and if you want to add new "slice" or instance, it can be added in 2 to 5 minutes. Amazon's Scalable Storage Service (S3) charges \$0.12 to \$0.15 per gigabyte-month and if you want additional bandwidth it charges \$0.10 to \$0.15 per gigabyte to move data from AWS over internet. Hence, Amazon states that by statistically multiplexing multiple instances on a single physical box, that box can be rented to many customers who will not interfere with each other (Armbrust et al., 2009, p5).

Armbrust (2009) calls this method of costing as "pay as you go". For instance, if you purchase hours from Cloud Computing, they can be distributed non-uniformly in time in the networking community i.e. uses 200 server-hours today and no server-hours tomorrow and pay for only what you use. Though this pay-as-you-go can be more expensive than buying a comparable server over the same period, but Armbrust argue that the cost is outweighed by the Cloud Computing benefits of elasticity and transference of risk. Regarding elasticity in Cloud Computing, the ability to add or remove resources at a fine grain (one server at a time) and along with used time of minutes rather than hours or weeks allows matching resources to workload more closely (Armbrust et al., 2009, p10). The server utilization of the real world estimates from 5% to 20% (Rangan and Siegel, 2008). This seems quite low, but it is an observation that the average workload for many

services exceeds by the factors 2 to 10. Some users deliberately specify for *less* than expected peak as they must specify the peak but in return they allow resources to be idle in the non peak times. This results in the waste of resources (Armbrust et al., 2009, p10).

There are other models also available in the market in consumer perspective. They have taken one of three forms i.e. *tiered pricing*, *per-unit pricing* and *subscription-based pricing* (Youseff et al., 2008, p7). Amazon cloud has adopted the *tiered pricing* model in which the cloud services are offered in several tiers and every tier provides fixed computing specifications (i.e. memory allocation, CPU type and speed etc.) and SLA (Service Level Agreement) at a certain price per unit time (Youseff et al., 2008, p7). *Per-unit pricing* is mostly used with data transfer and memory usage (Youseff et al., 2008, p7). GoGrid Cloud offering uses the main-memory allocation, where they denote “RAM/hour” as usage unit for their system (GoGrid, 2010). This method is more flexible than tiered pricing as it allows users to reallocate the memory location based on their needs. Finally the *subscription-based model* is mostly used for SaaS. This model lets the users to predict their periodic expenses of using Cloud Computing (Youseff, et al., 2008, p7).

2.2.2 COST IN PROVIDER’S PERSPECTIVE

For enterprises, in addition to investing the Cloud Computing cost, it is important to know the cost of providing Cloud Computing services because of couple of reasons. Firstly, there is a possibility that enterprises can’t legally migrate to public clouds, hence the use of private clouds become more important. Secondly, if enterprises once start private cloud, they can always rent out its spare IT space. Therefore, because of these reason it is good for enterprises to know the cost of having private cloud.

Some researchers have worked with the cost of cloud data centers. Greenberg et al. described how the cloud data center costs can be reduced by keeping in mind the cost of servers, infrastructure, power, and networking. According to them the costs can be reduced by running data centers at cooler temperatures to reduce cooling costs and building micro data centers to reduce bandwidth cost (Greenberg et al., 2009, p3).

2.2.3 CLOUD COMPUTING'S COST EFFECT

As I have already mentioned that Cloud Computing is an evolution from the Grid Computing, so we can say that most of the enterprises moved from Grid to Cloud. Hence, now I will study as how the enterprises are affected after moving from Grid to Cloud. In other words, I will see what Grid Computing had and what Cloud Computing possesses now to help the economics of enterprise.

2.2.3.1 BENEFITS

In a “Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS”, Khajeh-Hosseini et al. (2010a) talked about the third party cloud infrastructure. According to them if the third party cloud infrastructure is introduced then it presents many opportunities for enterprises to improve the management of income and outgoings for both finance staff and customers. It also helps the easing of cash-flow management for finance staff as the cloud pricing model has minimal upfront cost and monthly billing and it also lessens the variability of expenditure on electricity. These are the benefits comparing to the in-house data center, as it can be costly to buy hardware and cash-flow can also be slow and difficult from clients. Along with that energy costs will also go down as you are not running your own data center and third party cloud will be responsible for that. The Cloud infrastructure is also very helpful for the finance department of the company to reduce the administrative burden. Third party cloud infrastructure solutions offer new pricing models, which help in managing income for customers, sales and marketing staff (Khajeh-Hosseini et al., 2010a, p5).

Khajeh-Hosseini et al. (2010a) concluded that Cloud Computing is a disruptive technology that is set to change how IT systems in enterprises are deployed because of its cheap, simple and scalable nature. Cloud Computing can be significantly cheaper in comparison to buying and maintaining in-house data center as it eliminates the support related issues because there is no physical infrastructure to maintain. However, there are many social-technical issues which enterprises need to consider before migrating to Cloud (Khajeh-Hosseini 2010a, p7).

In any enterprise, the low level administrative costs can be quite high as the departments are scattered through in the building, often far greater than raw hardware costs. By the help of cloud, enterprises can offload three kinds of low level administration. First is system infrastructure which includes hardware maintenance, spare parts, adding new machines and infrastructure software is taken care by cloud. Second, once the enterprises define the backup policy, cloud provider is responsible to execute it. Lastly, a single application is installed once and becomes available to all authorized users. Though the management of the application i.e. application support, upgrade issues and user management is not included as moving to cloud does not change much in these tasks. It is important to note that the low level costs can be sometimes higher than the total cost for the cloud service (Rosenthal et al., 2009, p346).

In conventional systems, system resource utilization is low, estimated at 15–20 % for data centers; other estimates are lower (Evdemon and Liptaak, 2007). There are many reasons for low utilization as managers usually tend to buy for near peak and future loads and thus do not use the whole capacity all the time. While to help in this matter Cloud Computing smoothes these effects across many customers and today may attain 40 % (Vogels, 2008) utilization (Rosenthal et al., 2009, p346).

Server power is expensive because of processes like cooling and other overhead power consumptions. If combined together, they can be equal to the cost of one typical server used today. Cloud providers can do a lot better than typical server centers due to the better management of voltage conversions, cooler climates and better cooling, and lower electricity rates (cloud vendors tend to cluster near hydropower). Cloud providers are also usually located where real estate is cheap (Rosenthal et al., 2009, p346).

Rosenthal et al. (2009) in their article “Cloud Computing: A new business paradigm for biomedical information sharing”, discussed about the three major cost drivers of biomedical enterprises and how these are effected by the Cloud Computing technology. They include system administration, idle capacity, and power usage and facilities (Rosenthal et al., 2009, p346).

2.2.3.2 DRAWBACKS

Mayur et al. (2008) investigates the Amazon data storage service S3 for scientific data-intensive applications. According to them as S3 bundles at a single pricing method for all three data characteristics i.e. high durability, high availability and fast access but most of applications do not need all bundled together. For example, archival storage; which needs durability but can survive with lower availability and access performance. Hence, it is suggested that S3 should provide services through a number of limited classes of service so that users can choose their desired durability/availability/access performance mix to better costs (Mayur et al., 2008, p8). Hence, the cost is higher with storage service group durability/availability/access performance together.

In the report “Clearing the Air on Cloud Computing” by McKinsey & Co, they state that Cloud Computing can cost twice as much as in-house data centers. However, this is the issue only for large enterprises but small and medium sized enterprises are not affected by it and they get cost benefits. According to them” Cloud offerings currently are most attractive for small and medium-sized enterprises...and most customers of clouds are small businesses” (Lublinsky and Boris, 2009). The reason for this is that the smaller companies don’t have the option of developing themselves into giant data centers. Cost variability is a key aspect of Cloud Computing and when enterprises opt for cost transparency, scalability and cost variability, a new challenge and opportunity arises (Qamar et al., 2010, p2).

2.2.4 CLOUD COMPUTING VERSUS DESKTOP GRID

Cloud Computing has taken the commercial computing by storm. According to Kondo et al. (2009), the adoption of Cloud Computing by enterprises is in its infancy as performance and cost benefits are not clear, especially for desktop grids (volunteer computing). He compares the cost benefits of Cloud Computing for desktop grid applications. Cloud Computing provides easy access to company’s high performance computing and storage infrastructure through the web services (Kondo, et al., 2009, p1). Cloud Computing also hides the complexity of IT infrastructure management from its

users and provide massive scalability, reliability, high performance and specifiable configurability. All these capabilities are provided at a low cost comparing with dedicated infrastructure (Kondo et al., 2009, p1).

Both Cloud Computing and desktop grids have similar properties i.e. transparency. On both platforms, the users don't know where there tasks are executed. However, Cloud Computing infrastructure is different from desktop grids in both hardware and software but two main differences are configurability and quality of service. Cloud provides the configurable environment in terms of OS and software stack with Xen virtual machine forming the basis of EC2, while in desktop Grids, virtual machines are still in research (Kondo et al., 2009, p2).

Kondo et al. (2009) compared the cost benefits between these two platforms from the perspective of a parallel and compute intensive application. They calculated the desktop grid (volunteer computing) overhead for platform construction, application deployment, computer rates and completion times. According to them on average, hosts register at a rate of 124 cloud nodes per day and the ratio of volunteer nodes needed to reach the compute power of a small EC2 instance is almost 2.83 active volunteer hosts to 1 (Kondo et al., 2009, p10). The monthly cost of the desktop grid ranges from 5K to 12K and at the same time startup cost ranges from 4K to 43K. If we replace the desktop grids with Cloud Computing, pay per use costs will decrease by at least an order of magnitude.

The hybrid approach was also considered, where a VC server is hosted on the cloud to lower the startup and monthly costs and in result the savings ranges form 40 to 95 percent depending on the resource usage. Hosting on the cloud is cheaper if the bandwidth doesn't exceed 100Mbit and storage needs are less than 10TB's. Server bandwidth on EC2 cloud is more expensive (Kondo et al., 2009, p10).

2.3 CLOUD COMPUTING AND DATA SECURITY

This section deals with the data security issues related to Cloud Computing in the enterprise world.

2.3.1 DATA SECURITY IN CLOUD

As I have mentioned, because of the pay as you go method, most of the enterprises tend to move to Cloud Computing to save cost. The enterprises move to cloud and get the space for data storage. This data storage is certainly cheaper for them if compared to the in-house data storage but the question is, if this data storage in cloud is also secured and beneficial for enterprises. Hence, one of the most impending tasks for enterprises is the security of data storage. The IDC survey in Aug. 2008 has shown that security is the most serious concern for the enterprises ascribed to Cloud Computing (Gens, 2008).

To understand the security issue in Cloud Computing, it is important to know the architecture of Cloud Computing. Once you know the architecture of Cloud Computing then it becomes easier to understand the data security and privacy issues and also to figure them out. I have presented the architecture of cloud above in section 2.1.

Mostly the security issues which arise in Cloud Computing are the result of users/enterprises lack of control on the physical infrastructure. Enterprises mostly don't know where their data is physically stored and which security mechanisms are in place to protect data i.e. whether the data is encrypted or not and if yes, which encryption method is applied also if the connection used for data to travel in the cloud is encrypted and how the encryption keys are managed (Window Security, 2010).

Jensen et al. (2009) presented the technical security issues in Cloud Computing, however, these issues are more related with the problems of web services and web browser and not of Cloud Computing. These issues are still very important to Cloud Computing as Cloud Computing makes a lot of use of web services and users rely on web browsers to access the services offered by the cloud. The common attacks on web services include the XML Signature Element Wrapping, where XML signature is used for authentication (Jensen et al., 2009, p3).

Browser Security is also an important issue in Cloud Computing as in a cloud most of the computation is done on remote servers and the client PC is only used for I/O, and

authorization of commands to cloud. Hence, standard web browser was a need of situation to send I/O and this was utilized by different names: web applications, web 2.0 or Software as Services (SaaS). However, the use of web browser raised the question of security. TLS (Transport Layer Security) is important in this matter as it is used for host authentication and data encryption. XML signature or XML encryption cannot be used by browser directly as data can be only encrypted through TLS and signatures are only used with the TLS handshake. Hence, browser only serves as a passive data store (Jensen et al., 2009, p4).

As stated above, understanding the relationships and dependencies among Cloud Computing models is critical for understanding the security risks of it. For all the cloud services IaaS is the foundation and PaaS is build on it, while SaaS is build on PaaS and IaaS as described in the cloud reference model diagram (Cloud Security Alliance, 2009, p18).

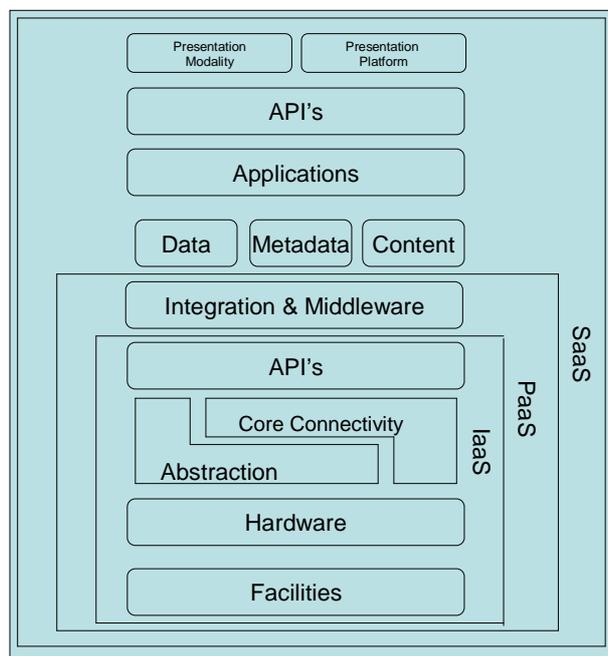


Figure 2 - Cloud Reference Model (Cloud Security Alliance, 2009, p18)

Security controls in Cloud Computing are not different than security controls in IT environment. However, as Cloud Computing deploys different service models, operation models and technologies, so it presents different risks to an organization. The enterprise security is implemented on one or more layers ranging from the facilities (physical security), to the network infrastructure (network security), to the IT systems (system security), and all the way to the information and applications (application security). The security responsibilities of provider and consumer are dependent on cloud models. For instance amazon’s AWS EC2, IaaS offering, has vendors responsibility for managing physical, environmental and virtualization security. On the other hand consumer is responsible for security at IT system level i.e. operating system, applications and data (Cloud Security Alliance, 2009, p25).

We can illustrate this issue by the help of a diagram, which shows how security structure responsibilities for different models vary (Cloud Security Alliance, 2009, p26).

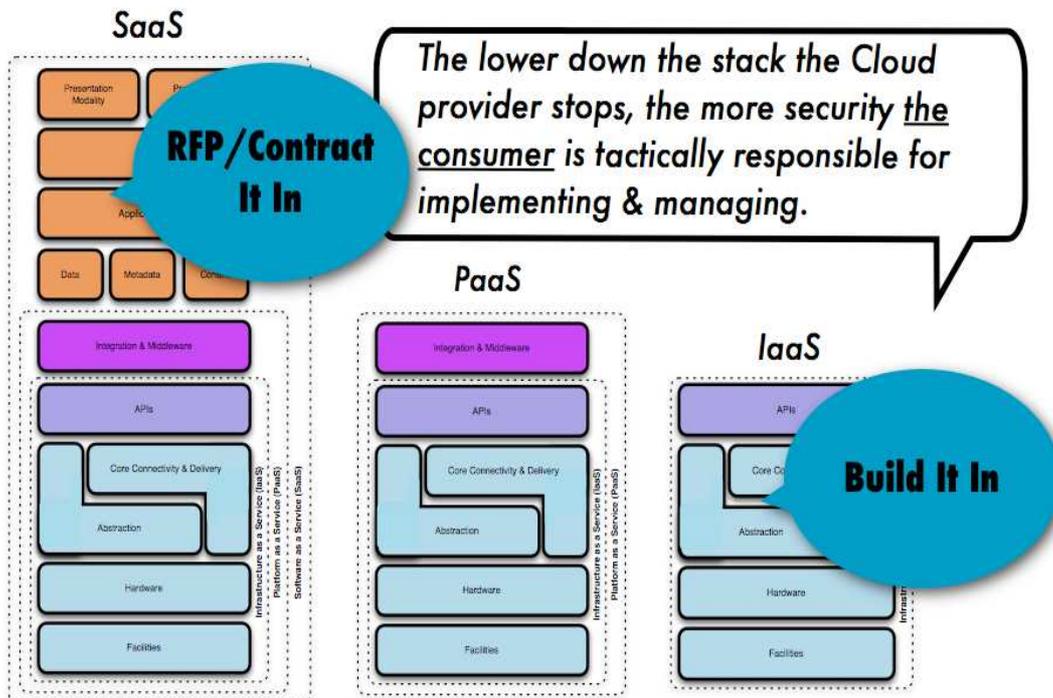


Figure 3 – How Security Gets Integrated (Cloud Security Alliance, 2009, p26)

It is very important to understand differences between service models to manage risk posture of the enterprise.

According to CSA, except architecture, there are also some other areas which should be considered while addressing the security issue in Cloud Computing. These areas can be divided into 2 parts i.e. *Governance Domains* and *Operational Domains*.

Governance domains are broad and tackle strategic and policy issues within Cloud Computing environment, whereas the operational domains address more tactical security concerns and implementation within the architecture vary (Cloud Security Alliance, 2009, p26). Governance Domains include:

- *Governance and Enterprise Risk Management*
It deals with the ability of organization to governing and measuring enterprise risk caused by Cloud Computing. It tackles with the issues like legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data and how international boundaries can affect these issues.
- *Legal and Electronic Discovery*
It addresses the legal issues when enterprises adopt Cloud Computing i.e. protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws etc.
- *Compliance and Audit*
It is about maintaining and proving compliance when enterprises move to Cloud Computing.
- *Information Lifecycle Management*
It deals with the management of data which resides in the cloud i.e. items surrounding the identification and control of data in the cloud, compensations controls which can be used to deal with the loss of physical control, and who is responsible for data confidentiality, integrity and availability.

- *Portability and Interoperability*

It discusses the movement of data from one provider to another or bringing it back to the enterprise.

And the Operational Domains consist of:

- *Traditional Security, Business Continuity and Disaster Recovery*

This takes into account as how the operational processes and procedures used to implement security are affected by Cloud Computing. This section also focuses on the risks of adopting Cloud Computing, in hopes for better enterprise risk management model.

- *Data Center Operations*

It discusses the evaluation of provider's data center and architecture as what are the common data center characteristics for long term stability.

- *Incident Response, Notification and remediation*

It addresses the items that should be in place at both provider and user levels to ensure proper incident handling and forensics.

- *Application Security*

It talks as how to secure the application software which is running in the cloud or being developed in cloud. This includes the choice if to move to cloud and if yes then which cloud platform should be adopted i.e. IaaS, SaaS, or PaaS.

- *Encryption and Key Management*

It identifies the proper encryption usage and scalable key management. It more talks about as why the encryption and key management should be used, both for protecting access to resources as well as for protecting data.

- *Identity and Access Management*

It discusses the management of identities and leveraging directory services to provide access control. It also takes into account the assessment of an enterprise's readiness to conduct cloud based Identity and Access Management (IAM).

- *Virtualization*

It discusses the use of virtualization in Cloud Computing. It discusses the risks associated with multi-tenancy, VM isolation, VM co-residence, hypervisor vulnerabilities etc. It also discusses the security issues related to only system/hardware virtualization (Cloud Security Alliance, 2009, p26-28).

The European Network and Information Security Agency (ENISA) also worked with the security issues in Cloud Computing and provided the most critical security risks while adopting Cloud Computing and which should be kept in mind before switching to Cloud Computing. They presented 35 risks which are involved with the security while adopting Cloud Computing (Catteddu and Hogben, 2009, p23). These 35 risks can be divided into the following categories:

- Policy and organizational risks such as vendor lock-in, loss of governance, compliance challenges, and cloud provider acquisition.
- Technical risks such as data leakage, distributed denial of service attacks, loss of encryption keys, and conflicts between customer hardening procedures and cloud platforms.
- Legal risks such as data protection and software licensing risks.
- Risks not specific to the cloud such as network problems, unauthorized access to data centers, and natural disasters (Catteddu, and Hogben, 2009, p24).

2.3.2 SECURITY BENEFITS OF CLOUD COMPUTING

I have talked about the data storage issues in Cloud Computing however; one must also look into the benefits of data storage in Cloud Computing. Craig Balding in his blog ‘Assessing the Security Benefits of Cloud Computing’ talks about these benefits. He advocates that there are some technical security arguments in favor of Cloud Computing assuming that we can find the ways to manage the risks.

European Network and Information Security Agency (ENISA) have also researched on the benefits for enterprises adopting Cloud Computing. Cloud Computing has a lot of

potential to improve security for enterprises and the ways it can improve security is described below.

Benefits of Scale

It is a fact that all types of security measures which are implemented on a larger scale are cheaper. Hence by adopting Cloud Computing enterprises gets better protection with same amount of money. The security includes all kinds of defensive measures such as filtering, patch management, hardening of virtual machine instances, human resources and their management and vetting, hardware and software redundancy, strong authentication, efficient role-based access control and federated identity management solutions by default, which also improves the network effects of collaboration among various partners involved in defense (Catteddu, and Hogben, 2009, p17). Along with these benefits, other benefits include:

Multiple Locations:

The cloud providers by default have economic resources to replicate content and this increases the redundancy and independence from failure. Hence, it provides the disaster recovery.

Edge Networks:

Cloud Computing provides reliability, quality increase and less local network problems for enterprises by having storage, processing and delivery closer to the network edge.

Improved Timelines of Response (incidents):

Cloud providers have larger to incidents or well-run-larger-scale systems. These systems help in improved timelines of response e.g. because of the early detection of new malware deployments, it can develop more effective and efficient incident response.

Threat Management:

The small enterprises don't have resources to hire specialists for dealing with specific security issues but cloud providers can do that and provide better threat management (Catteddu, and Hogben, 2009, p17).

Security as Market Differentiator

For most of the enterprises security is the most important issue while moving to Cloud Computing. They make choices on the basis of reputation of confidentiality, Cloud Computing benefits, risks and recommendations for information security integrity and resilience and security services offered by provider. This drives Cloud Computing providers to improve the security to compete in the market (Catteddu, and Hogben, 2009, p17).

Standard Interfaces for Managed Security Services

Standardized open interfaces to managed security services (MSS) providers are often provided by the large cloud providers. This offers more open market for security services where customers can choose or switch providers more easily with lower setup costs. Hence, the more resources can be scaled in a granular way without taking care of the system resources, the cheaper it gets to respond to sudden peaks in demand (Catteddu, and Hogben, 2009, p18).

Rapid, Smart Scaling of Resources

There are already many cloud resources including storage, CPU time, memory, web service requests and virtual machine instances which can be rapidly scaled on demand and as the technology is improving granular control over resource consumption is increasing. The cloud provider also have the resources and the rights to dynamically reallocate resources for filtering, traffic shaping, encryption etc, when an attack (e.g. DDoS) is likely or is taking place, to increase support for defensive measures. Hence, the cloud providers can limit the effect that some attacks have on the availability of resources that legitimately hosted services use by the combined use of dynamic resource allocation and appropriate resource optimization methods.

Therefore the ability to dynamically scale the defensive resources on demand has resilience benefits for enterprises. Furthermore, the more the scaling of resources in a granular way, the cheaper it is to respond to sudden peaks in demand (Catteddu, and Hogben, 2009, p18).

Audit and Evidence-Gathering

On demand cloning of virtual machines is supported by IaaS (Infrastructure as a Service), hence if a security breach occurs, the customer can make an image of a live virtual machine for offline forensic analysis. This can benefit in less down time for analysis. Furthermore, with storage on top, multiple clones can be created and analysis is performed in parallel to reduce investigation time. This gives benefit in improving the ex-post analysis of security incidents and increasing the probability of tracking attackers. Cloud Computing also provides cost-effective storage for logs hence, offering comprehensive logging (Catteddu and Hogben, 2009, p18-19).

Better Risk Management

The management of various risk scenarios in SLA (Service Level Agreement) and the impact of security breaches on reputation motivate the cloud providers for more internal audits and risk assessment procedures. This helps in exposing risks which would not be discovered otherwise, having in return some positive effects (Catteddu and Hogben, 2009, p19).

Resource Concentration

Concentration of resources has disadvantages for security without any doubt but it also has obvious advantages of cheaper physical parameterization and physical access control (per unit resource) and cheaper application of a comprehensive security policy and control over data management, incident management, patch management and maintenance processes (Catteddu and Hogben, 2009, p19).

Effective Updates and Defaults

In Cloud Computing the virtual machine images and software used by customers can be updated with latest patches and security settings along with that IaaS cloud service APIs allow snapshots to be taken of virtual infrastructure and compare it with baseline. Updates can also be rolled out many times more rapidly on the platform. PaaS and SaaS are also updated or patched on the centralized location. All of these are the benefits in implementing the better security (Catteddu and Hogben, 2009, p20).

Craig Balding is a system/database administrator after graduating from university with a Systems Analysis degree in 1994. He has ISC (Information Systems Security) certification. He is also ISACA i.e. Certified Information Security Auditor and Chartered IT Professional. Balding (2008) presents seven technical security benefits for enterprises. Some of them are immediate benefits while others may arrive with time and have some conditions attached. Cloud offers major security benefits to small and medium enterprises as most of them suffer with limited or non-existence in-house resources and budgets (Balding, 2008). The seven technical security benefits presented by Balding (2008) basically *strengthen* the above talked benefits and they include:

i. Centralized Data

One of the main security benefit provided by Cloud Computing is the centralized data. The benefits of centralized data are *reduced data leakage* and *better monitoring*.

Reduced data leakage is the most talked and popular benefit from the Cloud providers for enterprises. Most of the enterprises save their data on tapes and laptops but they are never secured. It is more secured to transfer data in the form of temporary caches or handled devices than transferring through laptops. Also not all small enterprises are using encryption techniques. Hence, the data can be made more secured with the use of Cloud Computing technology.

It is also easier to control and monitor data through central storage. However, on the other side it is also risky to have all data at one place as if theft happens, all data is lost but Balding prefers the centralized data. It is better to spend time on designing the security for one centralized place rather than figuring out the way to secure all the places where companies reside their data (Balding, 2008).

ii. Incident Response/ Forensics

By the use of Infrastructure as a Service (IaaS), it is possible to build a dedicated forensic server in the cloud as of in the enterprise and place it offline, ready for use anytime. One only needs to pay for storage and if an incident happens, enterprise just brings it online from the Cloud provider's web interface rather than calling someone to bring it online or install some boot server.

Evidence acquisition time is also decreased if enterprises decide to adopt Cloud Computing. For instance, if a server in the Cloud gets compromised, one can clone the server and make it available instantly to Cloud Forensics server.

Cloud Computing is beneficial in eliminating or reducing service downtime. As mentioned above one don't need to go to someone to tell them that system should be taken offline because of the abstraction of hardware by Cloud Computing providers. Hence, abstracting the hardware removes a barrier to even doing forensics in some situations.

The evidence transfer time is also decreased in Cloud Computing for enterprises. In the cloud bits to bits copies are super fast because of the replicated, distributed file system. It is also free to make copies in the cloud because of the network perspective. Without the cloud one must invest lot of time and expensive provisioning of physical devices.

Cloud Computing eliminates the forensic image verification time by implementation of cryptographic checksum or hash. For instance, Amazon S3 generates MD5 hash automatically when one stores an object hence; there is no need to generate time consuming MD5 checksums using external tools. Immense CPU power through Cloud Computing decreases time to access protected documents. One can test a wider range of different passwords in less time to speed investigation (Balding, 2008).

iii. Password Assurance Testing (Cracking)

The enterprises usually test password strengths regularly by running password crackers which is a time consuming process. However, this password cracking time is decreased by the use of Cloud Computing as Cloud providers do it by themselves. Another benefit of using cloud is keeping cracking activities to dedicated machines. Usually enterprises use distributed password cracker to spread the load across non-production machines but with cloud you place them on dedicated Compute instances (Balding, 2008).

iv. Logging

Cloud Computing provides another benefit for enterprises in the form of unlimited storage for logs. By the help of these logs in the cloud, enterprises can leverage cloud compute to index these logs in real time and get better and fast search results.

Enhanced logging is another beneficial aspect of Cloud Computing. Most of the modern operating systems offer extended logging system in the form of C2 audit trail but this is usually not used by enterprises because of performance degradation and log size issues. However, with Cloud Computing you can 'opt-in' easily if you are willing to pay for extended logging (Balding, 2008).

v. Improved State of Security Software (Performance)

Cloud Computing drives vendors to create more efficient security software. In cloud all billable CPU cycles get noticed hence, more attention will be paid by enterprises to inefficient processes e.g. poorly turned security agents. Therefore process accounting will make a comeback and vendors will go for improved security software (Balding, 2008).

vi. Security Builds

Pre-hardened, change control builds are another benefit of Cloud Computing. This is primarily a benefit of virtualization based Cloud Computing. Now one can start secure by creating the Gold Image VM and clone away. It will also reduce exposure through patching offline as Gold images can be kept securely up to date. While offline VM can be easily patched ‘off’ the network.

It is also very easy to test impact of security changes on cloud. Enterprises just need to make a copy of their production environment, implement a security change and then just test the impact at low cost with minimal startup time. This removes a major barrier of doing security in production environments (Balding, 2008).

vii. Security Testing

Cloud Computing provides reduced cost of testing security. With SaaS, the providers only ask for a portion of security testing costs to enterprises as they are sharing the same application as a service. Hence, you don’t pay much and save cost (Balding, 2008).

2.4 SUMMARY

In a nutshell we can say that cost and security are the important factors for any enterprise to adapt Cloud Computing.

Enterprises tend to choose the payment methods for paying Cloud Computing providers. Most common payment method for enterprises and the cloud providers is “pay as you go”. This is one of the novel feature of Cloud Computing, which is cheaper in a longer term

than having own data center. However, Cloud Computing is cheaper for small and medium sized enterprises than large enterprises. Elasticity is another factor for enterprises to adapt Cloud Computing as they can use their resources dynamically. Amazon S3 provides services in a bundle of high durability, high availability and fast access however most enterprises don't need all but some of them. Hence, cloud providers should work on it to give enterprises more benefit. The administrative costs are lessened with the adoption of Cloud Computing for enterprises.

Security of data is the most serious concern of enterprises adapting Cloud Computing. Most security issues are due to lack of control of enterprise over physical infrastructure. Web services and web browsers are also a concern regarding Cloud Computing as most of the cloud services are accessed through web. The security responsibilities of providers and consumers are dependent on cloud models e.g. Amazon's AWS EC2, IaaS offering, has vendors responsibility for managing physical, environmental and virtualization security. On the other hand consumer is responsible for security at IT system level i.e. operating system, applications and data. The lower down the stack the cloud provider stops, the more security the consumer is tactically responsible for implementing and managing.

Except architecture, governance and operational domains are also important in data security of cloud. The governance issues include Governance and Enterprise Risk Management, Legal and Electronic Discovery, Compliance and Audit, Information Lifecycle Management, and Portability and Interoperability. While the Operational issues include Traditional Security, Business Continuity and Disaster Recovery, Data Center Operations, Incident response, Notification and remediation, Application Security, Encryption and Key Management, and Virtualization.

Along with security concerns there are also some benefits of Cloud Computing with respect to security. These benefits include benefit of scale with multiple locations, edge networks, improvised time line of response, and threat management. Other benefits include security as market differentiator, standard interfaces for managed security

Cloud Computing effect on Enterprises

services, rapid and smart scaling of resources, audit and evidence gathering, better risk management, resource concentration, and effective updates and defaults. Like these Balding has also mentioned seven benefits of Cloud Computing including centralized data, incident response, password assurance testing, logging, improved state of security software, security builds and security testing.

3. RESEARCH STRATEGY

As I have already identified my subject and my research question, it is now important to match the design and methods with the problem statement and the research questions, in other words, a research strategy. The research strategy is the scientific method that helps answering the research questions. I will first observe an overall presentation of the strategy, with the research methods, the data collection analysis tools, investigating tools, ethics and so on. As mentioned, I have to identify what kind of research questions I have, to choose the right research strategy.

3.1 METHOD SELECTION

The method is a tool to generate solutions to problems and to derive new knowledge (Lekwall & Wahlbin, 2001). As Marshall & Rossman present three conditions to choose any strategy either experiment, survey, archival analysis, history or case studies, I have followed those three conditions i.e. a) the type of research questions posed, b) the extent of control an investigator has on actual behavioral events and c) degree of focus on contemporary events to choose my strategy (Marshall & Rossman, 1989, p5).

The first thing I considered was the research question. The research questions could be identified with three purposes as explanatory, descriptive or exploratory (Marshall & Rossman, 1989, p3). As Marshall, Rossman, and Yin said in their respective literature, the “what” questions leads to exploratory studies and “how” and “why” questions lead to explanatory studies (Marshall & Rossman, 1989, p3-6). As my question was to find the answer of what are the benefits and drawbacks of Cloud Computing, and the factors that shove the enterprises to shift to Cloud Computing technology, so the study I have pursued is exploratory case study (Marshall & Rossman, 1989, p6). I was aware of the essential variables of the subject, the phenomena, Cloud Computing, information systems in enterprises, cost effect, security effect and how they affect the enterprises. I had the basic constructs, thus I answered to the questions and gathered as much data as possible, and hence, I had more information. This is why the question began by “what”. The

question helped me to understand the phenomena in a particular context, Cloud Computing and enterprises. Hence, I also intended to get the answer of how the Cloud Computing works, so this lead to exploratory study. Therefore, my question was both exploratory and this lead to case study approach. Along with that, as I had no control over behavioral events and I wanted to focus on contemporary events thus case study approach was the best approach for my study and I pursued it (Marshall & Rossman, 1989, p5).

I have conducted multiple case studies one in Fox Mobile Group (Cloud Computing user) and second in DNS Europe (Cloud Computing provider) and have analyzed the results on a specific framework or theory to check the benefits or drawbacks for enterprises adapting Cloud Computing in regards with cost, and data security. I selected Fox Mobile Group to conduct my case study because they were using Cloud Computing in their company. I did not choose more enterprises for the case study because of the lack of resources. Another reason to choose FMG enterprise was, because I was employed there for an internship and it was easier to get contract for case study and information from people. Though I understood the point of biasness, however, I assured to be unbiased as I didn't work in Cloud Computing department. Hence, conducting interview in FMG was same as of some other enterprise.

The case study had been the most used and common research strategy to conduct a research. A case study is an empirical inquiry that “investigates a contemporary phenomenon within its real-life context, (Yin, 2002). The phenomenon in my case was of the different applications of enterprises running on cloud. Therefore the case study was an appropriate strategy for my research, which was quite important and really suitable for my research, by the quality of the information I get. The first case study was focused on one enterprise i.e. Fox Mobile Group and one certain application being run on cloud. The second case study was focused on the Cloud Computing provider i.e. DNS Europe, and how they managed and satisfied the needs and demands of the enterprises.

Concerning the study, one of the first steps was to create a study protocol. The goal of a study protocol was to collect data from a single case or a single respondent. It showed

step by step how the data was collected and helped anticipate problems. The study protocol included the context and the perspective of the specific study, the field procedure, and case study questions. It helped focus on the right questions related with the enterprise and their use of Cloud Computing, to get to right conclusions. I didn't want to get an answer on personal feelings about the way the information system of enterprise is working and about the usage of Cloud Computing in information system of the enterprise as my study is technical based so I focused on the real outcome of system rather than the feelings. This tool could be interpreted as a preparation for the data collection, but it was necessary for a guarantee of an accurate data collection.

Moreover, I conducted interviews in my case study as interview helped me in getting the desired information. I gathered a great deal of information regarding my scope (described above) of Cloud Computing. An interview is a conversation that has a structure and a purpose (Kvale, 1996, p6). According to Preece (2002), there are four types of interviews structure: unstructured, structured, semi-structured and group interviews. The first three relate to how much control interviewer has on the conversation by following a predetermined set of questions, while the fourth consists of a small group which is guided by an interviewer who facilitates a discussion of a specified set of topics (Preece et al., 2002). To decide the most appropriate approach the most important factors were evaluation goals, the questions to be addressed and the method of research adopted. If the goal was to gain an overall impression of a subject, then an informal, unstructured interview was often the best approach. However, if the goal was to get feedback about a specific issue then structured interview was better (Preece et al., 2002). I followed the seven stages of interview research which include Thematising (formulating the purpose of an investigation and describe the concept of topic to be investigated before the interview starts), Designing (plans the design of the study keeping in mind all the seven stages of investigation before the interview starts), Interviewing (conduct the interview based on an interview guide), Transcribing (prepare the interview material for analysis i.e. from oral speech to written text), Analyzing (choosing the appropriate method for analysis based on purpose and topic of investigation and the nature of interview material),

Verifying (ascertain the generalizability, reliability and validity of interview findings) and Reporting (having the result in readable form) (Kvale, 1996, p88).

As I have adopted a qualitative method and my aim was to get both the overall understanding of the information system of enterprise and Cloud Computing along with the perceived benefits and drawbacks related to them, hence, the most appropriate method was to conduct semi-structured interview.

Kvale (1996) described different types of interview questions which include introducing questions, follow-up questions, probing questions, specifying questions, direct questions, indirect questions, structuring questions, silence, interpreting questions (Kvale, 1996, p134). The crucial point of interviews was the formulation of the question, so I could get the information I need. Otherwise I would have got biased in the answers, and they would have been inaccurate for my study. Hence, I used all these types of interview questions in my semi-structured interviews.

The first interview I conducted in FMG focused on the Cloud Computing and the cost effects on enterprises. I formulated my interview guide which can be found on Appendix A. I started with introduction questions followed by general view of Cloud Computing. After the general questions I developed specifying and direct question about the cost effect on enterprises related with my theory part i.e. cost model, enterprise size, elasticity and administration cost etc.

The second interview with the same employee of FMG focused on security issues of Cloud Computing for enterprises. In this interview I started with the general questions about security and following with the specific questions like implementation of security, data connection encryption, TLS, security for different models of Cloud Computing, and governance issues. I also formulated the questions around the benefits offered to enterprise by Cloud Computing including centralized data, audit and effective updates. The interview guide can be found on Appendix B.

The third interview was done with the cloud provider DNS Europe and it focused on the provider's perspective of Cloud Computing. The interview was more of a general interview about both the cost and security effects on enterprise present in the real market. The interview can be found in Appendix C.

Once I conducted the interviews the next stage was converting the interview from speech to text. I recorded the interviews with a tape recorder which is a common way to record interviews now days (Kvale, 1996, p 160). Transcription reliability and validity was an important issue to take care of. I insured the reliability by asking a friend to transcribe the same interview from speech to text and then compare with mine as suggested by Kvale (Kvale, 1996, p 163).

3.2 DATA ANALYSIS

Once the data collection process was achieved, next step was data analysis. There were many methods which make the data analysis more meaningful. These techniques could be used to manage the interview text, to compress the interview in the form of some short sentences in order to get the important points said in the interview. Depending on the data collection methods and tools that I used, I chose to select the case study analysis to analyze my data.

It was very important during analysis to understand the textual data. One should highlight and understand the important part of a text to be able to comprehend the general meaning and then interpret it to bring coherence and sense. Hence, to achieve that I have pursued a circular process, I understood the text as a whole, and then interpreted parts of the text so I can have a better understanding of the whole, and back to the parts, and so on. In my study since I conducted multiple case studies, I was confronted to different people involved with Cloud Computing. Therefore, I encountered contradictory, incomplete, cloudy, and confused view on the interaction issue with information system and Cloud Computing technique. But with this approach to make sense of the whole picture, that is the relationship between the information system of an enterprise and Cloud Computing, it helped me to understand the textual data in a better way.

The case study analysis' goal was to make a very precise description of the case and its setting. In my case, effects of Cloud Computing in enterprises, the benefits and drawbacks in respect with the cost enterprises have to pay and their data security. I studied all the data, as I collected it, to be able to establish an outline, concerning each step in the processes described above. Inside the case study analysis method, I had some tools at my own disposition.

Direct interpretation: the principle of this tool was to select a precise instance, a single one, and try to find out the meaning of it, without cross checking or having multiple sources available to help (Creswell, 2007, p156-157). In my case, this process helped me to establish a stronger meaning to my issue, when I placed back together all the understanding that I found.

Then, I established patterns among my different cases (Yin, 2002, p26). By finding similarities and differences, I was able to determine a link between my cases and interpret them as a whole to create a general knowledge about the issue. The interpretation of different cases can take many meanings; it can be different persons that I interviewed and different study of information systems on the same issue. Hence, by this I decided what the cases were, and with the help of this method I found links among them.

Furthermore, I developed naturalistic generalizations from the data I analyzed. This was a generalization that the cases show to the people so they could learn it, and apply to another set of population (Creswell, 2007, p163).

It was clear that my form of writing the report for the study should be in relation with the strategy, the data collection and the data analysis. But first there were a few points that need to be discussed in order to deliver a suitable, credible and reliable report.

First, I did the reflexivity and representation in writing the report. The researchers cannot be distanced from the report, since we have a deep involvement in it; we have to assume

the consequences (Creswell, 2007, p179). Hence, I as a researcher explained my situation and the context in which I was writing the report. Since everything that happened around me affected me and it affected my interpretation. Therefore, the report that I have produced is a representation of what I experienced during a precise laps of time, and thus it cannot be acknowledged as a universal reference defying the law of space and time. I had the duty to inform the readers so they can have a better understanding of the overall study and interpretations I made. I also had to be aware of the participants feeling about the report, to see how they react to it, it is important be able to hear all the voices of a qualitative study.

Second, I had to be aware of the audience I was writing the report for (Creswell, 2007, p180). My primary audiences were teachers and researchers in the Information Systems field, and also students who were consulting my work for further studies. Hence, the report was shaped in a suitable form that let the audience have an easy understanding and critical judgment on my report.

Third, I had identified my audience, so I focused on encoding my writings. This meant that I had to choose my words carefully and in respect to the audience. Since my audience was mainly in the educational field, I used academic writing for my report (Creswell, 2007, p181).

Now that I decided different tools and tips for my report, I concentrated on the overall structure of the case study report. The structure was a case study structure report. This approach was suggested by Stake (1995) in Creswell book, (Creswell, 2007, p183-184) and from my point of view fits perfectly with my type of study.

I began my report by identifying the issue, Cloud Computing and the information systems in enterprises, and the purpose of the study. After that I concentrated on to find out if it was beneficial for enterprises to use Cloud Computing to have an efficient and effective information system in terms of cost and security, and finally the method of the study.

Next, I presented a full description of the case and its context. Then I presented the issues that were being studied in the precise context, this was from my understanding or from different literature that I came across and from which I made references. Then I investigated some of the issues, at this point I began to confirm or discredit the evidence I gathered, so that I could begin to interpret it.

Next, I presented statements, and a summary of what I understood about the case, my interpretation, and I discuss the conclusion being naturalistic generalization, so the reader can judge for himself.

I end the case, or/and the report, by a closing vignette, and not to forget that this case as I said earlier, was specially conducted in a space and time that cannot be reproduced.

3.3 RESEARCH QUALITY

In respect with the ethical issue, the first concerned I had was to respect the informed consent principle. I think it was crucial that during my study, each person that I encountered and who participated to the study should understand the purpose of the study and agree voluntarily to participate.

The second principle was the confidentiality. Inside the enterprises, I may be put in front of confidential experience or use of a certain information systems. In this case I got a formal agreement about dealing with certain information. I also informed every participant that everything confidential I see will not be exposed if they don't want to. But to be able to write my report in a way that won't be affecting them or me, I debated on which information they wish, and not wish to see inside my report. It may happen that a disagreement occurs, and in this case I shall favor the dialogue between the respondent and me. I also covered the real names and data of the interviewees, so they won't be recognize in any way.

The third principle was about avoiding harm and doing well if possible. My first concern was to be careful to do no harm that was psychological, or physical to the respondents. It

could be by exposing some of the data, or during an observation having them failed because of me. But in the end I tried to make my study contribute to their cause and if possible help them in any way possible to accomplish greater think concerning the interactional relation issue with the information systems.

The last principle was the relationships, integrity and ethics of care. During my study I made sure that my relations with the respondents were based on integrity and trust. A good way to do so was to let them know at each step of my study, what I had and what I intended to do. This was also very important if I had to make changes, in the research questions, of anything else. The respondents were an active part of my study, and a regular communication was established.

As I have mentioned earlier, I have worked in FMG and there were chances that I can be biased. However, as I didn't work in the cloud computing department therefore I am new to it and not biased. In case of validity, I sent my interviews transcripts to the interviewee to validate them.

4. EMPIRICAL STUDY

In this part of the thesis I have talked about the empirical study I carried out and its findings. I conducted my empirical keeping in mind the main research question i.e. what are the perceived benefits and drawback regarding cost and data security for Enterprises to adopt Cloud Computing? To answer this question the most suitable and appropriate contacts were the enterprises which are using Cloud Computing and the Cloud Computing providers for these enterprises.

4.1 INTERVIEWS

I found Fox Mobile Group in Berlin, an enterprise which is using Cloud Computing and can give answers of what benefits and drawbacks they are obtaining by adopting Cloud Computing. I conducted couple of interviews there with an employee responsible for Cloud Computing. As I mentioned before the reason to choose Fox Mobile Group was easy and difficult at the same time because I did internship there which resulted in easier access to the contact person and information but also getting biased and over through some critical information. However, I tried to maintain the balance as I know how important it is for research. On the other hand, I was also successful in finding a Cloud Computing provider named DNS Europe. I conducted the interview with them about the benefits and drawbacks they think enterprises can achieve with their adoption of Cloud Computing.

4.1.1 CLOUD COMPUTING AND COST

The first interview was conducted with an employee of Fox Mobile Group named X. The purpose for this first interview was to get to know about the company and its work. This interview was targeted to the cost effect (benefits and drawbacks) of Cloud Computing in enterprise. Mr. X is an IT team leader and responsible for the developer team. In his developer team they are responsible for developing music services on one side and on the other side so called acquisition engine, which is a server that hosted landing pages and record statistics. He described Fox Mobile Group as a global leader in mobile content

distribution, production and services, offering more of the benefits of mobile entertainment to consumers and business partners than anyone else. A division of News Corporation's Digital Media Group, FMG distributes and produces more mobile entertainment to more people and business partners in more ways and in more places than anyone else in the world. Its headquarter is in Berlin, Germany and Beverly Hills, Calif., Fox Mobile Group is wholly-owned by News Corporation (NASDAQ: NWS, NWSA; ASX: NWS, NWSLV). The main area where fox mobile is working is mobile entertainment products including ring tones, wallpapers, music, games range covering new smart phones and older devices. It's a medium sized enterprise.

According to the interviewee, FMG started using Cloud Computing with acquisition engine project. It was developed by an external software company and the company chose to deploy it in the Amazon cloud and it was the requirement from their strategy. However, the decision to put the application in cloud was of Fox Mobile Group. It was from the beginning of the project deployed in the cloud. The interviewee defined the Cloud Computing as *“Cloud computing is a flexible way to allocate resources out of a pool, enabling to consume processing power according to your needs. It makes easy to set up and decommission server instances, allowing the size of your infrastructure to grow when you need to address peaks while saving costs when you do not need the extra power anymore. The global usage of a cloud leads to the optimization of resources so that in the end it makes them cheaper for everybody involved”*. For this project the FMG is using IaaS (Infrastructure as a Service) because this is the model that fits best to their needs. They use the cloud as an infrastructure where they deploy their own application. They are using IaaS from Amazon which is being managed by a third party company named Right Scale. When asked about the reason to choose the specific cloud provider the interview replied that Amazon is a major player on this market, so it makes it obviously a candidate. It has benefited from its own internal needs for scalability and infrastructure flexibility and they continually extend their offer. In regards with the procedure to start working with Cloud Computing and the contract and legal issues, the interviewee was of the view that it is fairly straightforward to create an account and set up a server. There is plenty of ready to use server images that covers the need for

different setups like Web, Application or databases Server. That said, the team that created the infrastructure had to write a fairly amount of scripts to tailor the environment.

Before the adoption of Cloud Computing the FMG had exclusively been using the services of a classical datacenter. Mr. X was of the view that the location of data and the security requirements around them are obviously important issues and datacenter standard compliances and SLAs address them. Of course, deploying in the cloud kind of emphasizes the question about data security. But cloud does not mean automatically security problems. We are in the first place responsible for making our application secure. That said, we need sometimes some standardized compliances at enterprise level. Because we plan to deploy more in the cloud in the future, we are discussing an enterprise agreement with Amazon. When asked about how they were catering the daily demand before moving to cloud, the response was quite straight forward as it is a new application and its their first experience.

Along with testing, cost was one of the main factors for FMG to move to cloud. However, at the same time the interviewee told that cost was not the first factor to adopt Cloud Computing. The first reason was to give the team a complete autonomy on their deployment needs, allowing controlling the whole lifecycle of their activities. Cloud Computing is definitely more cost effective but costs were not the biggest reason in this case. The motivation in the first place was a new way to work for the team, a process to make them independent especially regarding their deployment and scalability needs.

FMG pay for every hour per machine, hence they follow “pay as you go” model and they are happy with it. According to interviewee it’s quite beneficial for them as it provides them flexibility. He was also of the view that they will not go for a private cloud, in the sense of setting up a cloud infrastructure on their own as he didn’t expect saving costs that way. However, they might go for something like a virtual private cloud to connect their cloud setup to their classical infrastructure via a virtual private network. Mr. X defined elasticity as capacity up and down. The obvious advantage of this is on the cost side; when we need more resources for a limited period of time, we only have to pay for

the extra power in this limited period of time. He stated it as one of the advantages and one of the reasons for adopting Cloud Computing.

FMG had no particular problem related to being in cloud so far hence, they said they are satisfied. However, they need to automate their deployment process just like the way they have done it in their process so far. Also they have to work a bit on their own on the monitoring of their application, what otherwise has been part of their standard processes in their classical datacenter infrastructure. In the cloud their team is responsible for itself. FMG did not opt for Grid computing before Cloud Computing as it is a new application which is developed in recent past however; they have used virtualized resources in their data center so Cloud Computing is a next step. When the interviewee was asked that durability, high availability and fast access are provided in a bundle from many cloud providers but some applications don't need them all and did your application need those all and If not then how is Cloud Computing cost effective? According to him considering their application they need high availability and performance but he could imagine for other profiles of application that you might want to choose the quality of services you need. He thinks it is very specific for application and they are happy for all these as they need all in their own specific application. Another benefit which the interviewee stated was that the system administration is lessened through the ability of loading a server image with the operating system and the software we need is just a mouse click away. And every developer in the team is able to do it. Sure it goes along with a couple of things developers have to take care of. All in all, it is cost effective.

4.1.2 CLOUD COMPUTING AND DATA SECURITY

The second interview was conducted with the same employee of the Fox Mobile Group as of the first interview. The purpose for the second interview was to get to know about the security of enterprise and security effect of Cloud Computing in enterprise i.e. Fox Mobile Group.

The first question asked to him was if the company i.e. FMG thought of the security issues before moving to Cloud Computing and is Cloud Computing secured for you at

enterprise level. According to him, Security is probably one of the questions that kind of worry people who are new to cloud. His team took over an application that was already deployed in the cloud. Nevertheless, as it was new to them, one of their infrastructure engineers did a small survey about that topic. They also looked at the documentation provided by Amazon about their security standards. They concluded that the security in the cloud primarily depends on the way you tackle security issues at the level of your server. The cloud is not a bigger threat as such when it matters to deal with the security at your application level (i.e. authenticating and authorizing access) or configuring which ports should be opened. At infrastructure level, they rely on Amazon and they feel they have tremendous experience here.

As the security was an issue for the enterprise my next question was if they did implement the security by themselves in the enterprise. They did not implement the security on the enterprise level for the certain application in the cloud. Apart from security at application level, their developer teams rely on their infrastructure team for security questions regarding networks, firewall, and protocols allowed to access servers or data in their standard datacenter. The data is not encrypted and he was worried about the place where data is stored. Regarding the encrypted connection, they had the connection encrypted. They use HTTPS for the communication between their frontend application deployed in the cloud and their API applications which are deployed in their standard datacenter. Also, the access to their APIs implies that the client uses a SSL client certificate they issued.

FMG rely on the protocols supported by the application server or the underlying operating system. As FMG is using IaaS of Amazon EC2 cloud and security is the responsibility of both the sides i.e. enterprise and cloud provider in the form of Physical security, Network Infrastructure, IT systems and Application security, hence, they take physical security as part of the service so they assume that no body can connect from the cloud to their server from a private address because it should be something restricted only for Amazon technical staff. However, they do take care of security at IT system level i.e. web security and planning to do more. FMG did not think of governance issues while adopting Cloud

Computing including Governance and Enterprise Risk Management, Legal and Electronic Discovery, Compliance and Audit, Information Lifecycle Management, and Portability and Interoperability. This is because the decision was taken to deploy only application which has no sensitive data so if someone could access their database they will see some product numbers but they wouldn't be able to see the price paid for the thing. Hence, it is more of a testing phase.

Fox Mobile Group does not think benefit is the added value of Cloud Computing and it is not one of the promises of the concept Cloud Computing. Hence, he did not think that anyone would say that I am going to cloud because I am more secured instead they will say I am going to cloud because it is scalable. However, he was of the view that security will become better because of market differentiator. Interfaces managers, are another benefit of Cloud Computing. It is nothing that the enterprises do normally in their data center. It is like ports configuration and access web mail with key. The interviewee was of the view that logging is helpful but he did not have concrete use case that I could make interesting comment out of it whereas FMG relies on the updates provided by Cloud Computing providers and it is helpful. They expect to benefit from a strict and well-organized update policy and a continual process that keeps the infrastructure at the most current level regarding security updates.

The interviewee described the FMG case about Cloud Computing as something to learn about cloud. He stated that security is always something one has to consider at the level of their application. One thing is sure when you are in the cloud you have theoretically less control than when you are in your own server or private network. Hence, he thought that it is more their own duty to make it more secured than to depend on others. Hence, they can configure firewall in cloud, limit access; e.g. they close every port except 80. He was of the view that it can be for marketing that cloud provider say that it is more secure but he thought its enterprise decision and duty to make and implement security. Hence, he was not sure about the future of cloud security if it will get better or not.

4.1.3 CLOUD COMPUTING AND PROVIDER'S PERSPECTIVE

Once the interview with the FMG i.e. users of Cloud Computing was done, it was time to see the other side of the picture, in other words, have the cloud provider's view. Hence, for that reason I consulted DNS Europe which is a cloud provider company and conducted an interview regarding my research question to know what they think and tell enterprises about the benefits an enterprise can achieve by adopting Cloud Computing. Along with that I tried to ask them about the drawbacks of Cloud Computing and how infant is the technology till today, which was of course a hard thing to get to know.

The interview was conducted with an employee of DNS Europe named Y. He is currently Chief Technical Officer at Cloud Computing services provider DNS Europe and is based full time in Belgrade, Serbia. I conducted the interview over the phone because of the distance problem. The purpose of the interview was to have the view of Cloud Computing providers as what they think is Cloud Computing, how infant the technology is what benefits they are offering to enterprise and what drawbacks according to them are still in the technology in terms of cost and security. According to the interviewee, DNS Europe is a pan-European IP Communications business that offers clients across Europe bespoke Internet-based services and solutions ranging from ISP system integration to product development and consultancy.

Mr. Y was of the view that Cloud Computing in the business world is the new thing which everybody is focused on and because of Cloud Computing everybody is also really focused on supply and management and most of this supply and management comes in and around the topic of security and compliance. Hence, the main thing which is holding back lots of enterprises when it comes to traditional Cloud Computing services is the security. As in the current model of cloud services it is very difficult to track where their data is physically stored. In other words it violates almost every provision and requirement for most of the information security auditors i.e. where their data is residing, and who has access to the physical machines.

Cloud Computing effect on Enterprises

Talking about the benefits the interviewee considered that there are many benefits of Cloud Computing and cost is one of them. Another huge benefit of the cloud is the efficiency and scalability which is provided through virtualization. For instance, the enterprises can scale now to what they require. By the help of Cloud Computing now enterprises don't have to spend capital expenditures i.e. they don't have to do big equipment purchases, they don't have to try and speculate before the business is even established as what their growth is going to be like, and what their scaling to be like. Rather, by adopting cloud model they can essentially say that they can start smaller and scale up to whatever they need. After scalability next thing is flexibility which is offered by Cloud Computing as a strong benefit, for instance one has got disposable infrastructure which means one do not have to buy servers. Hence, you can take an environment out and can put it in the cloud before you take any decision of your investment.

The interviewee also told about the trends of the market as how the enterprises solve their technical issues keeping in mind the Cloud Computing technology. According to him most of the enterprises which are getting around the Cloud Computing limitation, they start using private clouds. Private cloud is exactly the same as Amazon or Google except it's based on the hardware that people own themselves. For instance, for DNS Europe, it works with the "Applogic", which is a cloud operating system, offered by "3Tera". 3Tera is just being acquired by computer associates and what they do is that they say you can take the commodity hardware all you need, put the cloud operating system and that essentially gives you your private cloud. With this approach one gets all the benefits of Cloud Computing which include virtualization, encapsulation, and ability to migrate application. Hence, by the use of this approach, enterprise information data security policy goes all the way down to physical layer.

DNS Europe offers both the private and public clouds to their customers. They are a Cloud Computing provider, although the private cloud is their own and they provide services from it. The interviewee described a typical use case of his company, for instance; a team of developers from either small or big company come to them and ask to

place a multi-tera application but they don't know if its going to work for them hence, it is an experimental build or testing phase. They don't have the ability to invest in hardware or in infrastructure; hence, their company provide them with end to end services. DNS Europe get requirements, analyze the basic of the application to help the customer build that application on the cloud and then deploy. They can also help them in managing and supporting it on the cloud. On the contrary Amazon has a different approach as they don't provide support apart from forum when they give their services to their clients. However, the reason for their success is that they provide rock bottom prices which no one can compete with. It is important to know that there are limited numbers of professionals not only in developers but also for system administrators for managing Cloud Computing. Hence, DNS Europe find customers who are lacking operating system, grid system or system administration level knowledge and have developing skills and then provide them with system administration. It is another benefit of cloud that developers do not have to think about system administration and other things and just code and develop.

There is a huge confusion among the terminologies used in Cloud Computing now days including IaaS, PaaS, and SaaS. Gartner has also just published about the rights and responsibilities about Cloud Computing services and it is like a manifesto for cloud providers. DNS Europe does not get too involved in these terminologies because ultimately they like to cover different levels of interactions of all three or more types of services which are available. DNS Europe tends to use different set of terminologies which are more functional base for people who are not familiar with Cloud Computing.

I asked the interviewee about the company site as it stated grid computing rather than Cloud Computing and according to him their site was going to be updated soon as when they started their company Applogic was grid computing and now the terminology has changed in the industry. According to the interviewee grid computing was strictly speaking the utility computing where the idea was to get resources on demand as you need. However, now people are jumping to Cloud Computing without actually knowing the right definition of it hence, if the company does not use the word "cloud", it is not

even in the running. Enterprises or people talk about on demand services as Cloud Computing for instance, if enterprise needs more resources we will throw a server for them, we will scale their application but these are on demand service not a cloud service. Hence, all things are getting mashed together under the umbrella of Cloud Computing which in turn lets enterprises not to care about cloud or grid and what they actually want is they have requirements and they want to have X hence, what is the cost and the benefits. So, it always comes down to lower level conversation. The interviewee stated that DNS Europe is going to stick as service provider and they think it is hard for them to compete with Amazon.

The interviewee while talking about the market trends told that enterprises are a bit reluctant to move to cloud, they do have it on their plans but they are more into moving to virtualization than to cloud. It is hard to find some enterprises moving their mails to Gmail, the reason for this is that they are too conservative. However, according to interviewee enterprises will try to look for ways to imitate it and that's why DNS Europe thinks that "private cloud" is an answer to it. The enterprises want to have the benefits of Cloud Computing but they don't want Gmail, they don't want their data to be living on the same hard disk as of any one else, they want to know where their data is actually residing and also they like to have that one is not dependant on a single hardware failure because of virtualization. Hence, most of cloud providers like GoGrid and ourselves; provide services as if enterprise loose hard disk, its trivial, that node takes itself out of it and the virtual machine running on it bring itself up again on another one. Enterprises love this idea and are looking in the direction of VDI, virtual desktop.

The interviewee thought that Cloud Computing is very beneficial for small and medium sized enterprises and it is going to flourish especially when various cloud services have inter-collaboration for instance, in social media where facebook is being able to authenticate with flicker and twitter. However, large enterprises are still not sure about Cloud Computing and have their reservations which in turn make private cloud very interesting for them. Private clouds and data centers are essentially the same thing where data centers are the subsets of all cloud services.

Cloud Computing usage face some legal issues according to the interviewee. Increasingly service providers are being audited for instance, DNS Europe customers demand that they want their compliance in place however, they want to do payments in credits cards from the cloud applications. Hence, they had their own policy but essentially what they did they copied and pasted DNS Europe information policy which is really a statement about what good things we do. In DNS Europe case we haven't been audited and haven't gone through the ISO certification however, we have to do it because as service providers we have to demonstrate how enterprises can do business with them when they don't have access to the information of enterprises. On the other hand the interviewee was of the view that it is difficult because almost all technologies allow the administrators to get in and have access to data on those cloud systems. All DNS Europe can do is that they can say, there is a ghost in the machine and system administrators but we have check and balances, we have got monitoring, we have our own change control procedures. In a nutshell, we do training at a personal level rather than at a system level. Hence, there are niggles and problems with contract but most enterprises are balancing those risks.

DNS Europe has cloud control panel which is coming out very soon, which gives people the ability to manage the virtual infrastructure on private clouds without having to be the owner of the private cloud.

4.2 INTERVIEWS DISCUSSION

The first think which I focused during my empirical study i.e. interviews was what is Cloud Computing for enterprises and cloud providers. Mr. X of the enterprise Fox Mobile Group defined Cloud Computing "Cloud computing is a flexible way to allocate resources out of a pool, enabling to consume processing power according to your needs. It makes easy to set up and decommission server instances, allowing the size of your infrastructure to grow when you need to address peaks while saving costs when you do not need the extra power anymore. The global usage of a cloud leads to the optimization of resources so that in the end it makes them cheaper for everybody involved". On the other hand, according to the employee Mr. Y of Cloud Computing Provider DNS Europe

Cloud Computing is a new thing on which everyone in the market is focused on and because of this they are also focused on supply-chain management. Efficiency and Scalability through virtualization can be achieved in Cloud Computing whereas private cloud is not a part of Cloud Computing. Both of these definitions given by Cloud Computing provider and user correspond to the definition by Barkley RAD in 2.1.1, which considers Cloud Computing as both the application delivered on internet and also the hardware and system software in data center that provide those services. Hence, it is the Sum of XaaS and utility computing where private cloud is an internal data center and not for public use. Therefore, there is a consensus in the market about the Cloud Computing definition among the users and providers of Cloud Computing and they understand the technology.

As I stated in 2.1.1 that one of the characteristics of Cloud Computing is that the infrastructure resources and applications are provided in X as a Service manner. Hence, I inquired about this with Fox Mobile Group. FMG are using IaaS (Infrastructure as a Service) because that model fits their demands. They are using Amazon Cloud (a major player in the market) which is being managed by third party named Right Scale. The main reason to run the project on IaaS is because they are medium sized company and don't have server capabilities to support this project also they wanted to give their developer team a complete anonymity on their deployment needs.

I think the first reason was to give the team a complete autonomy on their deployment needs, allowing controlling the whole lifecycle of their activities. However, on the other hand, the cloud provider was of an interesting view which is different from FMG (Cloud Computing user) and the theory stated. According to him there is confusion in the market regarding the technologies and models including IaaS, PaaS, SaaS used in Cloud Computing. DNS Europe does not get involved in these technologies and ultimately they like to cover different levels of interactions of all these models or more types of services which are available. The rationale for this is that DNS Europe mostly works with big enterprises who do not want to get involved in these terminologies and want private clouds. They just provide them their requirements and want the solution. Hence, they use

terminologies which are more functional base. This shows a different trend of the market in regards to the size of the company and its needs. However, again stating that private cloud is not a part of Cloud Computing and DNS Europe do sometimes use XaaS terminologies for medium and small sized companies depending on their demand. Therefore, I will conclude that XaaS is an essential part of Cloud Computing.

Another characteristic of Cloud Computing is virtualization, elasticity and dynamic scalability on demand. The enterprises take it as a benefit for themselves as according to the employee of FMG. Cloud Computing is quite beneficial for them as it provides flexibility, scalability or elasticity. Whereas, the Cloud Computing providers DNS Europe confirm this statement by stating that flexibility and scalability (elasticity) is a benefit of Cloud Computing which is provided through virtualization. He elaborated more by giving an example that enterprises can scale now to what they require. They do not have to spend capital expenditures to buy equipments and try to speculate the growth even before the start of the business; rather they can start smaller and scale up whenever they want. Hence, the architecture defined in 2.1.1 and 2.1.2 is to huge extent is agreed upon by both the Cloud Computing users (enterprises) and providers in terms of its definition i.e. new computing paradigm, infrastructure resources and application are provided in X-as-a-Service manner, elasticity, and virtualization and dynamic scalability on demand.

After the understanding of Cloud Computing, the next question which comes to everyone's mind is how this Cloud Computing evolved. I have discussed this issue in 2.1.3; the Cloud Computing evolved from Grid Computing. Grid Computing allowed allocation of multiple servers onto a single task or job however, Cloud Computing provided virtualization of servers i.e. one server to compute several tasks concurrently. Grid Computing was typically used for job execution i.e. the execution of a program for a limited time whereas Cloud Computing is mostly used to support long-running services. As mentioned by Foster et al. (2008), "The evolution has been a result of a shift in focus from an infrastructure that delivers storage and compute resources to one that is economy based aiming to deliver more abstract resources and services". The FMG enterprise

though never used Grid Computing but they have used virtualized resources in their data center and Cloud Computing is the evolution or next step for them. Hence, I was unable to confirm it. However, the employee of DNS Europe confirmed this evolution. DNS Europe previously had been providing Grid Computing to their customers since the start of the company and now they have moved to provide Cloud Computing which is evolution from Grid Computing. The proof of this is the website of the company which is still stating Grid Computing. However, according to the DNS Europe they are in the process of updating their site to Cloud Computing.

4.2.1 THE COST EFFECT

One thing that everyone hears with Cloud Computing is the cost and that is why I devised my research question to find out how Cloud Computing affects enterprises in terms of cost. During my interviews at FMG, I tried to find out how cost affects the enterprise in their business and if Cloud Computing is really cost effective. As stated in the theory 2.2 that the economic appeal of Cloud Computing is often mentioned as “converting capital expenses to operating expenses” (Armbrust et al. 2009, p12), the enterprises (FMG) consider Cloud Computing the same way. FMG stated that, except giving the development team complete autonomy the other reason was cost efficiency. There are different detailed cost/price models in the market for Cloud Computing (Khajeh-Hosseini et al., 2010b, p4) i.e. pay as you go, tiered pricing, per-unit pricing and subscription based pricing. The FMG also adopted one of the cost models named “pay as you go”, in which FMG pays for every hour they use. Hence, they purchase hours from Cloud Computing provider, which are distributed non-uniformly in time in the network community.

Now that we know about the price models which enterprises use, the next thing is to examine if these price models have any impact on cost and if they are beneficial or cost effective for enterprises. According to Armbrust this “pay as you go” can be a bit expensive than buying a comparable server over the same period. However, he also argued that cost can be outweighed by the Cloud Computing benefits of elasticity (Armbrust et al., 2009, p10). In the case of FMG they can not afford to buy servers as they are medium sized company and also they are in a testing phase and it does not make

sense to deploy a big infrastructure to test your application. The thing which compensated FMG is the elasticity factor of Cloud Computing and it has made it very cost effective for the enterprise. Therefore, FMG is very satisfied with the use of Cloud Computing and the cost effect on the enterprise due to elasticity, because they just pay for what they need at that the moment.

DNS Europe agreed with the statement that flexibility and elasticity factor makes Cloud Computing cost effective for enterprises. The employee of DNS Europe stated that through scalability or elasticity, the enterprises can scale now to what they require. By the help of Cloud Computing now enterprises don't have to spend capital expenditures i.e. they don't have to do big equipment purchases, they don't have to try and speculate before the business is even established as what their growth is going to be like, and what their scaling to be like rather, by adopting Cloud Computing model they can essentially say that we can start smaller and scale up to whatever we need. After scalability or elasticity, the next thing is flexibility which is offered by Cloud Computing as a strong benefit, for instance one has got disposable infrastructure which means you do not have to buy servers. Hence, you can take an environment out and can put it in the cloud before you take any decision of your investment. Hence, it is proven that elasticity makes Cloud Computing cost effective for the enterprises.

Apart from elasticity another factor on which cost of Cloud Computing effects is the size of the enterprise. In the report "Clearing the Air on Cloud Computing" by McKinsey & Co, they state that Cloud Computing can cost twice as much as in-house data centers. However, this is the issue only for large enterprises but small and medium sized enterprises are not affected by it and they get cost benefits. According to them "Cloud offerings currently are most attractive for small and medium-sized enterprises...and most customers of clouds are small businesses" (Lublinsky and Boris, 2009). FMG proved the statement correct as they are medium sized enterprise with not much demands and can not afford big data centers, hence through Cloud Computing they are saving cost. Hence, Cloud Computing is really cost beneficial for medium sized companies.

Now the question arises how Cloud Computing gets cost beneficial for medium and small enterprises. One argument which is already mentioned is that, the enterprises do not have to invest in buying big servers. The other argument was presented in 2.2.3 by Khajeh-Hosseini that when Cloud Computing is introduced then it presents many opportunities for enterprises to improve the management of income and outgoings for both finance staff and customers. It also reduces the administrative burden as it offers new pricing models which help in managing income for customers, sales and marketing staff (Khajeh-Hosseini et al., 2010a, p5). FMG was of the same view that the system administration is lessened through the ability of loading a server image. By that the operating system and the software you need is just a mouse click away. All in all, it is cost effective. Hence, with Cloud Computing the administrative burden for enterprises is reduced which end up in cost benefit.

There is another aspect which can prove to be beneficial or disadvantageous for the enterprises. Mayur et al. (2008) has investigated the Amazon data storage service S3 for scientific data-intensive applications. According to them as S3 bundles at a single pricing method for all three data characteristics i.e. high durability, high availability and fast access but most of applications do not need all bundled together (Mayur et al., 2008, p8). Hence, the companies which don't need all these three data characteristics, they don't have any choice than to pay for it. This makes it disadvantageous for them. However, during the empirical study, FMG required all these three characteristics for their application, hence, this aspect of the Amazon cloud is really beneficial for them.

Hence, it is summarized as:

- There are four factors which affect the cost factor of any enterprise. They include elasticity or scalability, flexibility, data center cost, pricing models, and administration cost.
- Cloud Computing is cost effective for enterprises in respect to these factors and is very beneficial for the medium and small sized enterprises.

4.2.2 THE SECURITY EFFECT

The second part of my research question related to the data security issues of Cloud Computing. During my empirical study I have tried to investigate if adoption of Cloud Computing with respect to data security is beneficial or a drawback for enterprises. As I have mentioned in 2.3 that to understand the security effect of Cloud Computing for enterprises, one have to understand the architecture of Cloud Computing. During my first interview with the employee of FMG, we discussed the architecture of Cloud Computing, which I have already mentioned. Therefore, I straight away started with the security affect on the enterprise FMG.

I started with a very general question i.e. did FMG thought of security issues before moving to Cloud Computing and is Cloud Computing secure enough for them. The FMG employee reiterated his first approach as stated in the first interview that it was the decision of the company who developed the application to deploy it in Cloud. However, once this application was handed over to them they did a research on that and came up with interesting results. As mentioned in 2.3.1 that most of the security issues that arise for enterprise through the use of Cloud Computing is due to the fact of lack of control on the physical infrastructure. Enterprises do not know where there data is resided and which security mechanism is applied to protect it i.e. whether the data is encrypted or not and if yes, which encryption method is applied also if the connection used for data to travel in the cloud is encrypted and how the encryption keys are managed (Window Security, 2010).

In the result of the research conducted by FMG, the one issue was the same i.e. no control over physical data storage and anonymity about the protection methods applied. The employee stated that the fact that one can access the jars and apis in the cloud worries them. They also don't know the route rights for the users granted by Cloud Computing provider. Before adapting Cloud Computing, FMG used to route the users for everything they do on the server and the infrastructure in their standard data center is configured according to roles and some have no route rights. Therefore, at the moment they are not keeping the transactional data in cloud. As they are at the starting stage and use of Cloud

Computing is very minimal, hence, FMG is not planning to implement any security yet. However, there is a new project ready to be deployed in the Cloud and for that they will certainly work with the security issues.

Except the anonymity of physical storage of data in Cloud Computing another issue is “Web Security”. Jensen et al. presented the technical security issues in Cloud Computing. These issues are very important to Cloud Computing as Cloud Computing makes a lot of use of web services and users rely on web browsers to access the services offered by the cloud. The common attacks on web services include the XML Signature Element Wrapping, where XML signature is used for authentication (Jensen et al., 2009, p3). Hence, to implement web security, FMG are not sure if their data is encrypted in the cloud by the cloud provider. However, the connection is encrypted. Their access to the services is over https as it is required. Hence, web security methods are applied and for use case they will setup a VPN in future.

More in Browser Security, Jensen et al. stated that it is an important issue in Cloud Computing as in a cloud most of the computation is done on remote servers and the client PC is only used for I/O, and authorization of commands to cloud. However, the use of web browser raised the question of security. TLS (Transport Layer Security) is important in this matter as it is used for host authentication and data encryption (Jensen et al., 2009, p4). FMG, understand this security concern and they rely on protocols (TLS) available in the app server and https with client certificates. While for access to their backend services they use client certificates like SSL.

The management of security in a cloud also depends on the Cloud Computing model an enterprise is using. As stated by Cloud Security alliance that for all the cloud services IaaS is the foundation and PaaS is build on it, while SaaS is build on PaaS and IaaS (Cloud Security Alliance, 2009, p18). As stated in 2.3.1 that the enterprise security is implemented on one or more layers ranging from physical, to network, to system and all the way to application security. Therefore, the security responsibilities of provider and consumer are dependent on cloud models. For instance Amazon’s AWS EC2, IaaS

offering, has vendors responsibility for managing physical, environmental and virtualization security. On the other hand consumer is responsible for security at IT system level i.e. operating system, applications and data (Cloud Security Alliance, 2009, p25). This concept was endorsed by FMG and as they are using IaaS, they acknowledged that the physical security is taken as part of the service from Amazon hence they assume that no body can connect from the cloud to their server from a private address because it should be something restricted only for Amazon technical staff. However, they do take care of security at IT system level.

According to CSA, except architecture, there are two areas on which enterprises should focus for security in Cloud Computing and they are *Governance Domains* and *Operational Domains* (Cloud Security Alliance, 2009, p26). In regards with FMG they did not take care of these areas as they decided to deploy non sensitive data on the cloud. In this case even if someone gets access to data, they will see nothing else but some product numbers which are not critical. However, during this interview they I told them about these domains and they agreed that an enterprise must follow them before adopting Cloud Computing and they will also consider these for their future plans.

In the end, the employee of FMG agreed with the European Network and Information Security Agency (ENISA), who have summarized all these issues in their report. These are 35 critical security risks, which should be kept in mind before adapting Cloud Computing (Catteddu, and Hogben, 2009, p23). As mentioned before, these include:

- Policy and organizational risks such as vendor lock-in, loss of governance, compliance challenges, and cloud provider acquisition.
- Technical risks such as data leakage, distributed denial of service attacks, loss of encryption keys, and conflicts between customer hardening procedures and cloud platforms.
- Legal risks such as data protection and software licensing risks.
- Risks not specific to the cloud such as network problems, unauthorized access to data centers, and natural disasters (Catteddu, and Hogben, 2009, p24).

The FMG employee stated that, at the moment during the starting stage of Cloud Computing in their enterprise they did not take care of all these issues. However, they were already planning to take care of them during their future projects in a cloud.

After the issues with the security of Cloud Computing we discussed the benefits. FMG was quite clear with their view about the benefits offered by Cloud Computing in security domain and he stated that he do not think benefit is the added value of cloud computing and its not one of the promises of the concept Cloud Computing. Hence, he do not think anyone would say that I am going to cloud because I am more secured instead they will say I am going to cloud because it is scalable. Hence, in this statement I can see that the enterprises are not so satisfied with the benefits offered by Cloud Computing in security domain. However, I have tried to find the brighter side of the security and I have also discussed it with the employee.

Besides these issues in Cloud Computing security, according to many professionals in the IT industry there are also many benefits of security in Cloud Computing. One of the main advantages for enterprises in terms of security is the benefit of scale. As stated by ENISA, it is a fact that on the large scale security is always implemented better and cheaper. Therefore, by adopting Cloud Computing enterprises gets better protection with same amount of money. These benefits include multiple locations by which data can be replicated on different locations, improved timelines of response, and better threat management as small companies cannot afford to hire security specialists (Catteddu, and Hogben, 2009, p17). FMG agrees with it to certain extent as they are also a medium sized company and can not afford people only for security solutions. The employee stated that it is certainly a fact that on a larger scale one can implement better security with less money. However, he did point out here that it is again about saving money. Therefore, even in the security benefit of Cloud Computing the cost factor is introduced which proves his first statement correct that security is not the added value of Cloud Computing.

Security gets better in Cloud Computing for enterprises because of market differentiator. Most enterprises make choices on the basis of reputation of confidentiality, Cloud Computing benefits, risks and recommendations for information security integrity and resilience and security services offered by provider. This drives Cloud Computing providers to improve the security to compete in the market (Catteddu, and Hogben, 2009, p17). FMG employee confirmed this and told that it will motivate the Cloud Computing to provide better security and in turn it will be a benefit for enterprises. Standard interfaces for managing security services are another beneficial characteristic of Cloud Computing. This offers more open market for security services where customers can choose or switch providers more easily with lower setup costs. Hence, the more resources can be scaled in a granular way without taking care of the system resources, the cheaper it gets to respond to sudden peaks in demand (Catteddu, and Hogben, 2009, p18). FMG is using that standard interface provided by Right Scale and it is helping them to manage their cloud in a better way. Hence, it is certainly a big advantage for the enterprises in terms of security management.

Audit and evidence gathering or logging is another added benefit of Cloud Computing for enterprises. On demand cloning of virtual machines is supported by IaaS (Infrastructure as a Service), hence if a security breach occurs, the customer can make an image of a live virtual machine for offline forensic analysis. This can benefit in less down time for analysis. This gives benefit in improving the ex-post analysis of security incidents and increasing the probability of tracking attackers. Cloud Computing also provides cost-effective storage for logs hence, offering comprehensive logging (Catteddu, and Hogben, 2009, p18-19). For the employee of FMG logging is a novel feature offered by Cloud Computing providers and helps the enterprises however, till now he do not have any concrete use case where the enterprise has made use of it. Nevertheless he was of the view that it will help them a lot in improving or maintaining security in future. Another benefit is the better risk management because of the SLA (Service Level Agreement) between enterprises and Cloud Computing providers. This motivates the cloud providers to do more internal audits and improve risk management procedures.

One of the most important benefits which enterprises obtain from Cloud Computing in terms of security is the effective updates in the cloud. In Cloud Computing the virtual machine images and software used by customers are updated with latest patches and security settings on the centralized location. This results in better security in the cloud for enterprises (Catteddu, and Hogben, 2009, p20). FMG considers it a very strong benefit as they also used to update their servers during the use of their data center. They are well aware with the importance of updates and are satisfied with this approach of Cloud Computing providers.

In the end, the most important benefit and also a disadvantage at the same time is the centralized data in Cloud Computing. The benefits of centralized data are *reduced data leakage* and *better monitoring*. Reduced data leakage is the most talked and popular benefit from the Cloud providers for enterprises. Most of the enterprises save their data on tapes and laptops but they are never secured. It is more secured to transfer data in the form of temporary caches or handled devices than transferring through laptops. It is also easier to control and monitor data through central storage (Balding, 2008). These all points stated by Balding shows the benefit however, the centralized data is also more prone to attacks. The employee of DNS Europe mentioned the same risk. However, at the same time the employee of FMG, DNS Europe and Balding agree that it is better to spend time on designing the security for one centralized place rather than figuring out the way to secure all the places where companies reside their data. Therefore, centralized data is a security benefit for enterprises in Cloud Computing.

Therefore, it is summarized from the above analysis that:

- Security benefits are not the added value of Cloud Computing.
- There are security issues because of lack of control on physical infrastructure.
- Web security is also a concern because Cloud Computing relies on web servers.
- Management of security in cloud is dependent on the model an enterprise is using.
- There are two areas on which enterprise should focus for security in Cloud Computing i.e. Governance Domains and Operational Domains.

Cloud Computing effect on Enterprises

- There are many benefits of security which include benefit of scale, market differentiator, standard interface, logging, effective updates, and centralized data.

5. CONCLUSION

In this research work, I tackled the affects of Cloud Computing in the enterprises. The specific areas I researched during my study were cost and security. I have found that Cloud Computing is a very hot topic now days and many enterprises are interested in it. Most of the enterprises have idea about it but still there is confusion about the real definition of Cloud Computing. This is understandable as this technology is in its infant stage however, as it evolved from Grid Computing therefore, most of the enterprises which have used Grid Computing are better able to understand the term Cloud Computing. There is a confusion or disagreement about the boundaries of Cloud Computing as many enterprises and even cloud providers believe that private cloud is a part of Cloud Computing. However, in my research I have found that *Cloud Computing is the sum of Software as a Service (SaaS) and Utility Computing, but does not include Private Clouds.*

The enterprises which are in the process of making a decision to adopt Cloud Computing face real dilemma as they hear different (positive and negative) views from different sources. The first characteristic that tends enterprises to think about Cloud Computing is the cost effect. I have done a thorough research about the cost effect on enterprises. There are many factors or characteristics which affect the cost of Cloud Computing for enterprises. These factors include elasticity, flexibility, data center cost, pricing models and administrative costs. The elasticity is the biggest factor to make Cloud Computing cost effective for enterprises and most of the enterprises move to cloud because of this characteristic of Cloud Computing. I have concluded that enterprises save their capital by not building their data center and not hiring employees for managing them. Along with that flexibility and different pricing models makes Cloud Computing more cost effective for enterprises. However, an important finding is that these benefits are only for medium sized or small enterprises. The large enterprises can save their cost by building big data center due their demand and capital they have. In other words, private cloud is something perfect for the large enterprises.

In my empirical study, I also managed results about the second part of my research question i.e. security in Cloud Computing for enterprises. Here I would like to mention the first response of my interview with the employee of FMG. He clearly stated that security benefit is not the added value of Cloud Computing. I have concluded that Cloud Computing have many security issues for enterprises. These issues include no control over physical data, web browser security, distributed denial of service attacks, loss of encryption keys, legal risks, network problems and natural disasters. However, along with these drawbacks there are some also some benefits for enterprises. These benefits are of scale, standard interface, logging, risk management, and effective updates and defaults. However, in my empirical study, I have concluded that these benefits do not overcome the security issues of Cloud Computing. Hence, enterprises should not adopt Cloud Computing because of better security for their data.

In a nutshell, I will conclude that Cloud Computing is emerging as a big and beneficial technology of present day and future. Much of work is being put in it and one can expect more progress in Cloud Computing technology. However, for enterprises the most important factor to adopt Cloud Computing will stay cost till today and security is still not the added value of Cloud Computing for enterprises despite its benefits. The most important finding is that the Cloud Computing is ideal for medium and small sized enterprises both in terms of cost benefits. However, in terms of security, it is not so beneficial for medium and small enterprises to adopt Cloud Computing. For large enterprises it is more effective to adopt private cloud because with private cloud they can save cost and have better security.

Appendix A: Interview 1

Purpose of the Interview

The purpose for this first interview is to get to know about the company and its work. This interview will be targeted to the cost effect of cloud computing in enterprise.

Questionnaire for the Interview

General Enterprise

- *What is your position and responsibilities in the company?*

I am responsible for developer team. We are responsible for developing music services on one side and on the other side so called acquisition engine, which is a server that hosted landing pages and record statistics.

- *What are the main areas of work of Fox Mobile Group? How big is the enterprise? You consider it to be large, medium or small?*

The main area where fox mobile is working is mobile entertainment products including ring tones, wallpapers, music, games range covering new smart phones and older devices. It's a medium sized enterprise.

- *I presume you are using cloud computing, When did the Fox Mobile adopt cloud computing?*

Fox started using cloud computing with acquisition engine project. It was developed by an external software company and they choose to deploy it in the Amazon cloud and it was the requirement from their strategy.

- *Whose decision was to move to cloud?*

It was decision of Fox Mobile Group. It was from the beginning of the project deployed in the cloud.

- *Can you please define cloud computing as what it is to you?*

Cloud computing is a flexible way to allocate resources out of a pool, enabling to consume processing power according to your needs. It makes easy to set up and decommission server instances, allowing the size of your infrastructure to grow when you need to address peaks while saving costs when you do not need the extra power anymore. The global usage of a cloud leads to the optimization of resources so that in the end it makes them cheaper for everybody involved.

- *Which cloud service are you using? IaaS, PaaS or SaaS? And why?*

We are using IaaS (Infrastructure as a Service) because this is the model that fits our needs. We use the cloud as an infrastructure where we deploy our own applications.

- *Which Cloud provider are you using?*

We are using Amazon and we manage our cloud infrastructure through third party Company named Right Scale.

- *Any specific reason to choose that provider?*

Amazon is a major player on this market, so it makes it obviously a candidate. It has benefited from its own internal needs for scalability and infrastructure flexibility and they continually extend their offer.

- *How did you get started with the cloud? Easy process? Legal procedures? Number of days to start working? Contract to be signed?*

It is fairly straightforward to create an account and set up a server. There is plenty of ready to use server images that covers the need for different setups like Web, Application or databases Server. That said, the team that created the infrastructure had to write a fairly amount of scripts to tailor the environment.

- *How was Fox dealing with its data, before cloud computing? If In-house data center → What were the issues in it?*

We had exclusively been using the services of a classical datacenter so far. The location of data and the security requirements around them are obviously important issues and datacenter standard compliances and SLAs address them. Of course, deploying in the cloud kind of emphasizes the question about data security. But cloud does not mean automatically security problems. You are in the first place responsible for making your application secure. That said, you need sometimes some standardized compliances at enterprise level . Because we plan to deploy more in the cloud in the future, we are discussing an enterprise agreement with Amazon.

- *According to you what were general/main factors to move to Cloud?*

I think the first reason was to give the team a complete autonomy on their deployment needs, allowing to control the whole lifecycle of their activities. Costs are another reason.

- *How were you catering before the daily demand of the application moved on cloud? Did you guess the peak hours?*

As I mentioned, it's a new application and also our first experience in Cloud.

Cost Effect

- *Is cloud computing more cost effective and is the cost biggest reason to move to cloud?*

It is more cost effective but costs were not the biggest reason in this case. The motivation in the first place was a new way to work for the team, a process to make them independent especially regarding their deployment and scalability needs.

- *Do you think “the cost model” is beneficial for enterprise and you are happy with it?*
- *Which costing model are you using with cloud providers? Pay as you go, tiered, per unit pricing, subscription based?*

We pay for every hour per machine hence, it is pay as u go.

- *As you are big company, why didn't you go for having private cloud and saving cost in longer term?*

No I don't think we will go for a private cloud, in the sense of setting up a cloud infrastructure on our own. I don't expect saving costs that way. What we might use is something like a virtual private cloud to connect our cloud setup to our classical infrastructure via a virtual private network.

- *Do you see any issues in Cloud computing so far?*

We had no particular problem related to being in the cloud so far. Hence, I can say we are satisfied. We need to automatize our deployment process just like the way we have done it in our process so far. Also we have to work a bit on our own on the monitoring of our

application, what otherwise has been part of our standard processes in our classical datacenter infrastructure. In the cloud our team is responsible for itself.

- *Are you aware with the elasticity factor of cloud? What do you think about it?*

Elasticity is scaling capacity up and down. The obvious advantage of this is on the cost side; when you need more resources for a limited period of time, you only have to pay for the extra power in this limited period of time.

- *Before cloud Grid was in the market, why didn't you opt for going for it?*

We have used virtualized resources in our datacenter. Cloud computing is kind of a next step.

- *High durability, high availability and fast access are provided in a bundle from many cloud providers but some applications don't them all. Did your application need them all? If not then how is cloud cost effective?*

Considering our application we need high availability and performance but I can imagine for other profiles of application you might want to choose the quality of services u need. I think its very specific for application. We are happy for all these as we need all in these applications.

- *System administration has been lessened by cloud? Does it make things cost effective for enterprise?*

System administration is lessened through the ability of loading a server image with the operating system and the software you need just by the mean of a mouse clicks. And every developer in the team is nable to do it. Sure it goes along with a couple of things developer have to take care of. All in all, it is cost effective.

Appendix B: Interview 2

Purpose of the Interview

The purpose for the second interview is to get to know about the security of enterprise and security effect of cloud computing in enterprise.

Questionnaire for the Interview

Security Effect

- *Did you think of security issue while moving to cloud computing?*
- *For your enterprise cloud computing is secured or not?*

Security is probably one of the questions that kind of worry people who are new to cloud. As I told you in the previous interview, my team took over an application that was already deployed in the cloud. Nevertheless, as it was new to us, one of our infrastructure engineers did a small survey about that topic. We also look at the documentation provided by Amazon about their security standards. We concluded that the security in the cloud primary depends on the way you tackle security issues at the level of your server. The cloud is not a bigger threat as such when it matters to deal with the security at your application level (i.e. authenticating and authorizing access) or configuring which ports should be opened. At infrastructure level, we rely on Amazon and we feel they have tremendous experience here.

- *Have you implemented the security by yourself in the enterprise?*

Apart from security at application level, our developer teams rely on our infrastructure team for security questions regarding networks, firewall, protocols allowed to access servers or data in our standard datacenter.

- *Do you know where your data is stored and does it make you worried?*
- *Do you know if your data is encrypted? If yes, which encryption method is applied?*

Our data are not encrypted.

- *Is the connection used for data to travel is encrypted?*

We used HTTPS for the communication between our frontend application deployed in the cloud and our API applications which are deployed in our standard datacenter. Also, the access to our APIs implies that the client uses a SSL client certificate we issued.

- *The https is done by you or cloud did it?*

We don't have any instruction or constraints imposed by cloud or their team. It is an application choice to communicate through https.

- *Do you implement TLS (Transport Layer Security)?*

We rely on the protocols supported by the application server or the underlying operating system.

- *In IaaS of Amazon EC2 security is the responsibility of both the sides i.e. enterprise and cloud provider in the form of Physical security, Network Infrastructure, IT systems and application Security. How do you manage it?*

Physical security is something we take as part of the service so we assume that no body can connect from the cloud to our server from a private address because it should be something restricted only for Amazon technical staff. We haven't done anything on our own regarding that.

- *Did you think of Governance Issues while adopting cloud computing including*
 - Governance and Enterprise Risk Management
 - Legal and Electronic Discovery
 - Compliance and Audit
 - Information Lifecycle Management
 - Portability and Interoperability

I think very basically the decision was taken to deploy only application which has no sensitive data so may be if you could access our database you will see some product numbers but you wouldn't see the price paid for the thing. Hence, it is more of a testing phase.

- *What do you think are the security benefits of cloud computing?*

I don't think benefit is the added value of cloud computing and its not one of the promises of the concept cloud. Hence, I don't think anyone would say that I am going to cloud because I am more secured instead they will say I am going to cloud because it is scalable. But that said, you benefit of large scale experience regarding security in datacenter and virtualized systems.

- *Do you think security of cloud becomes better because of market differentiator?*

Of course, it helps in a certain way.

- *How beneficial is the standard interface for managed security services for enterprises?*

Well these interfaces managers, it is nothing that we do normally in our data center. Its like ports configuration and access web mail with key.

- *Does evidence and audit get better with cloud computing i.e. logging?*

Yes logging is helpful but I don't have concrete use case that I can make interesting comment out of it.

- *Effective updates and defaults is a feature of cloud computing, do you think it makes data more secured?*

We expect to benefit of a strict and well-organized update policy and a continual process that keeps the infrastructure at the most current level regarding security updates.

- *Are you satisfied with the security provided by cloud providers? What do you expect in future to change in cloud regarding security?*

When I speak for our case I think there is something to learn about cloud. I think security is always something you have to consider at the level of your application. One thing is sure when you are in the cloud you have theoretically less control when you are in your own server or private network. Hence, I think its more our duty to make it more secured than to depend on others. But still we can configure firewall in cloud, limit access; we close every port except 80. But this is something you would do everywhere else than cloud too. I think it can be for marketing that cloud provider say that it is more secure but I think its enterprise decision to make and implement security. So, I can not tell you the future of cloud security.

- *Can you think of any improvements in the security of Cloud computing from the providers for enterprises to make them feel more secure?*

I think it is somehow available on Amazon. I think private network that you group your server instance in one private network. It's already a possibility for virtual private networks and I don't think right now any improvements accept what I told before.

Appendix C: Interview 3

Purpose of the Interview

The purpose for the third interview is to get to know about the cost and security effect of cloud computing on enterprises from cloud provider's perspective.

Questionnaire for the Interview

- *What is your position and responsibilities in the DNS Europe?*
- *What are the main areas of work of DNS? How big is the enterprise?*
- *Which sized companies you take care of?*

The interview was conducted with an employee of DNS Europe named Y. He is currently Chief Technical Officer at Cloud Computing services provider DNS Europe and is based full time in Belgrade, Serbia. I conducted the interview over the phone because of the distance problem. The purpose of the interview was to have the view of Cloud Computing providers as what they think is Cloud Computing, how infant the technology is what benefits they are offering to enterprise and what drawbacks according to them are still in the technology in terms of cost and security. According to the interviewee, DNS Europe is a pan-European IP Communications business that offers clients across Europe bespoke Internet-based services and solutions ranging from ISP system integration to product development and consultancy.

- *Can you please define cloud computing as what it is to you?*

Cloud computing in the business world is the new thing which everybody is focused on. And because of cloud computing everybody is also really focused on supply and management. Lot of this supply and management comes in and around the topic of pivety, security and compliance with many of the standards like PCI and many others.

And it's of course the main thing which is holding back lots of enterprises when it comes to traditional cloud services that's because the current model of cloud services, its very difficult to track where physically your data actually is. In other words this violates just about every provision or requirement most of the information security auditors like pci, i.e. where your data is, who has access to the physical machines and this is before you can get to logical layer. Hence, when it comes to cloud services it can be difficult for companies to answer that question. There are many benefits of cloud and cost is one of them. Another huge benefit of the cloud is the efficiencies. In other words, it's true because of virtualization as well. When people use what they need, in other words they can scale exactly to the size they require. Hence, cloud is giving people is that they don't have to do capital expenditures i.e. they don't have to do big equipment purchases, they don't have to try and speculate before there business is even established what their growth going to be like, what their scaling to be like however by taking cloud model they can essentially say that we can start smaller and we scale up to whatever we need. That's one of the main things as so called "breed able computing".

Testing phase

First thing is scalability and second thing is flexibility, because you have got disposable infrastructure which means I don't have to buy servers and all these things. I can take an environment out and I can put it in the cloud before I take any decision of my investment in it. There is very interesting thing which we also do. As most of the companies are getting around the cloud computing limitations, they start using private clouds. Private cloud is exactly the same as Amazon or Google except it's based on the hardware that people own themselves. For instance, for my company, it works with the "Applogic", which is a cloud operating system, offered by "3Tera". 3tera is just being acquired by computer associates. And what they do is, they say u can take the commodity hardware all you need, put the cloud operating system and that essentially gives you your private cloud. You got all the benefits of standard cloud computing, you have got virtualization, encapsulation, ability to migrate application to and from locations. Hence, by use of that there information data security policy goes all the way down to physical layer. We have

many people how say we like to use services but we can't because we got to control that and we need to know where exactly everything is placed and we cant have multi tenancy and we need to control every element of the stack.

- *At DNS you are providing the private cloud or also cloud computing?*

We offer both, we offer private clouds to the customer, we also in a sense offer our own Applogic grids or clouds and we resell those services so people can buy virtual infrastructure, machine applications which run on our clouds. Hence, in a sense we are also a cloud computing provider, although the private cloud is ours and we provide services from it. Typical use case would be: let's say a team of developers come to us and they need to put in place a multi-tera application and they might be a small or big company but they don't know whether its going to work or not and we want to have an experimental build. They don't have the ability to invest on hardware or in infrastructure. Hence they come to us and we and many other cloud providers provide an end to end services. So we can get requirements, analyze the basic of the application to help the customer build that application on the cloud and then deploy. We can also help them in managing and supporting it on the cloud. Amazon has a bit different approach as they say take this virtual machine and don't expect any support apart from the forum. But they can give you rock bottom prices which no one can compete with, so companies which want that kind of disposability they opt to that. You know that there is a limited number of the professionals not only in developers but also for system administration for managing cloud application. Hence, even people know how to code but they don't know how to run the infrastructure and how to run it. Hence, we find these kinds of customers who miss operating system, grid system or system administration level knowledge and they come to us and tell us we know to develop and all can you run the system below it. That's another benefit of cloud as developers don't have to think about the other things and just code and develop.

- *Which cloud service are you providing? IaaS, PaaS or SaaS?*

Often things confuse and overlap. There is a huge confusion about these terminologies and what exactly are these for instance IaaS can have PaaS and SaaS also in it. Gartner has also just published about the rights and responsibilities about cloud computing services and its like a manifesto for cloud providers. We don't get too involved in the IaaS or PaaS or SaaS because ultimately we can cover different levels of interactions of all three or more types of services which are available and can be delivered. We tend to use different set of terminology which is more functional base and we try to use those terminology for people who are not familiar with cloud computing might understand.

- *How can a company get started with the cloud? Easy process? Legal procedures?*
- *Number of days to start working? Contract to be signed?*

In a sense legal problems are there. Increasingly service providers are being audited. So they are sub audited by companies before they are audited. For instance our customers come and say we want our compliance in place we want to payments in credits cards from the cloud applications. So they had their own policy but essentially what they did they copied and pasted our information policy which is really a statement about what good things we do in order to make sure that we don't completely destroy it. In our case we haven't been audited, we haven't gone through the ISO certification yet but we are going to have to. As service providers have to demonstrate how enterprises can do business with us without us having access to their information. But it is difficult because almost all technologies allow the administrators to get in and have access to data on those cloud systems. This is about which most enterprises are worried about. All you can do is, you can say there is a ghost in the machine and system administrators but we have check and balances, we have got monitoring, we have our own change control procedures. So we do training at a personal level rather than at a system level. So there are niggles and problems with contract. Hence most enterprises are balancing those risks.

- *How would u differentiate data center and private cloud?*

Essentially it's the same thing. Data centers are the subsets of all cloud services.

- *Why are you using term grid computing on your site and not cloud computing?*

Actually in 2 days time our site is going to republished. When we started Applogic was grid computing but now the terminology in the industry changed. Grid computing was strictly speaking the utility computing. The idea was you get resources on demand as you need and that was what original grid computing. But now people are jumping to cloud without knowing what exactly it is. As you mentioned already it is not cloud what people call it. There is a narrow definition of cloud. But now if you don't use the word cloud then you are not even in the running. For instance, people talk about on demand services as cloud for example if you need more we'll through a server for you, we will scale your application but that's on demand service not a cloud service. Hence, many things which are happening are all getting mashed together in the umbrella of cloud computing and it's hard for people to differentiate what they are. So enterprises actually are not caring whether it is grid or cloud but what actually they want is they have requirements and they want to have X, so what are the costs and what are the benefits. So it always comes down to lower level conversation. Hence, we are going to stick as service providers and we think it's hard to compete as Applogic with Amazon. It's too early to invest into it. The only things which make people interested is the thing that people are coming up with the noble ideas competing with one another. Also enterprises are bit reluctant to go to cloud now. They have it on their plans and they are more into moving to virtualization than to cloud. I don't think you will find many enterprises moving their mails to gmail. I think they are too conservative but what I think they will do is they will start to look for ways to imitate that and that's why we think that private cloud might be more interesting. They'll say fine we don't want gmail, we don't want our data living on the same hard disk as of Rehan or Jonathan data, who knows where is this google's data center is, may be in Africa or Pakistan. So they will say we will like to have benefits of clouds, we like to have data security, we will like to have that you are not dependant on a single hardware failure because of virtualization. With most of cloud providers like goGrid and ourselves, if you loose a hard disk, it's trivial, that node takes itself out of it and the virtual

machine running on it bring itself up again on another one. They love these ideas. Enterprises are also looking in the direction VDI, the virtual desktop.

I think for small and medium sized enterprises cloud make so much sense and this is going to flourish. Especially when various cloud services have inter-collaboration, we see it in the social media space when facebook being able to authenticate with flicker and twitter. I think large enterprises like the idea but they are not sure about it hence, the idea of private cloud suits them.

- *Do you have interface for the users?*

We have cloud control panel which is coming out very soon, which gives people the ability to manage the virtual infrastructure on private clouds without having to be the owner of the private cloud.

REFERENCES

Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2009). *Above the Clouds: A Berkeley View of Cloud Computing*. Technical Report. University of California at Berkeley.

Balding C. (2008). *Assessing the Security Benefits of Cloud Computing*. Cloud Security Blog, available at <http://cloudsecurity.org/blog/2008/07/21/assessing-the-security-benefits-of-cloud-computing.html> . Accessed 10th May, 2010.

Boss, G., Malladi, P., Quan, D., Legregni, L., Hall, H. (2007), *Cloud Computing*. www.ibm.com/developerworks/websphere/zones/hipods/. Retrieved on 20th May, 2010.

Catteddu, D. and Hogben, G. (2009). *Cloud Computing: benefits, risks and recommendations for information security*. Technical Report. European Network and Information Security Agency.

Creswell, J. W. (2007): *Qualitative inquiry and research design : choosing among five traditions*. 2nd ed., Sage Publications, Thousand Oaks, Calif.

Cloud Security Alliance. (2009). *Security Guidance for Critical Areas of Focus in Cloud Computing*.

Creeger, M. (2009). "CTO roundtable: cloud computing," *Comm. of the ACM*, vol. 52.

Evdemon J, Liptaak C., (2007). Internet Scale Computing: MSDN Blog, Oct 17, 2007. Available at: <http://blogs.msdn.com/jevdemon/archive/2007/10/24/internetscale-computing.aspx>.

EGEE (2008) An EGEE Comparative Study: Grids and Clouds – Evolution or Revolution? Enabling Grids for E-science (EGEE) report, 11 June 2008. <https://edms.cern.ch/document/925013/>. Accessed 1st May 2010

Fellowes, W. (2008). *Partly Cloudy, Blue-Sky Thinking About Cloud Computing*. Whitepaper. 451 Group.

Foster I, Kesselman C (1998) Computational Grids. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.36.4939>

Foster I, Kesselman, C, Tuecke S (2001) *The Anatomy of the Grid: Enabling Scalable Virtual Organization*. *International Journal of High Performance Computing Applications* 15(3):200-222

Foster I, Zhao Y, Raicu I, Lu S (2008) *Cloud Computing and Grid Computing 360-Degree Compared*. In: Grid Computing Environments Workshop (GCE'08). doi:10.1109/GCE.2008.4738445

Gens, F., (2010). "IDC on 'the Cloud': Get Ready for Expanded Research", <http://blogs.idc.com/ie/?p=189> . Accessed May 10, 2010.

Gartner (2008). *Gartner Says Cloud Computing Will Be As Influential As E-business*. Gartner press release, 26 June 2008. <http://www.gartner.com/it/page.jsp?id=707508>. Retrieved 3rd May 2010

GoGrid, (2010), <http://www.gogrid.com>. Accessed April 11, 2010.

Gleeson, E. (2009). *Computing industry set for a shocking change*. Retrieved May 10, 2010 from <http://www.moneyweek.com/investment-advice/computing-industry-set-for-a-shocking-change-43226.aspx>

Greenberg, A., Hamilton, J., Maltz, D. and Patel, P. (2009). *The Cost of a Cloud: Research Problems in Data Center Networks*. ACM SIGCOMM Computer Communication Review, 39, 1.

Harris D (2008) Why 'Grid' Doesn't Sell. On-Demand Enterprise blog, 24 March 2008. <http://www.on-demandenterprise.com/blogs/26058979.html>. Accessed 20 August 2009

Harms, U., Rehm, H-J., Rueter, T., Wittmann, H. (2006) *Grid Computing für virtualisierte Infrastrukturen*. In: Barth T, Schüll A (eds) *Grid Computing: Konzepte, Technologien, Anwendungen*, pp. 1-15. Vieweg+Teubner, Wiesbaden

Jensen, M., Schwenk, J. O., Gruschka, N. and Iacono, L. L. (2009). *On Technical Security Issues in Cloud Computing*. In IEEE International Conference on Cloud Computing (CLOUD-II 2009), Bangalore, India, September 2009, 109-116.

Joseph J, Ernest M, Fellenstein C (2004) *Evolution of Grid Computing Architecture and Grid Adoption Models*. IBM Syst. J. 43(4):624-644

Khajeh-Hosseini, A., Greenwood, D., Sommerville, I., (2010a). *Cloud Migration: A Case Study of Migrating an Enterprise IT System to IaaS*. Submitted to IEEE CLOUD 2010

Khajeh-Hosseini, A., Sommerville, I., Sriram, I., (2010b). *Research Challenges for Enterprise Cloud Computing*. Submitted to the 1st ACM Symposium on Cloud Computing, SOCC 2010.

Kondo, D., Javadi, B., Malecot, P., Cappello, F., Anderson, D., (2009). *Cost-Benefit Analysis of Cloud Computing versus Desktop Grids*. INRIA, France, UC Berkeley, USA.

- Kourpas E (2006) *Grid Computing: Past, Present and Future – An Innovation Perspective*. IBM white paper.
- Kvale, S. (1996) *Interviews: an introduction to qualitative research interviewing*, SAGE, Thousand Oaks, CA.
- Lekwall, P., and Wahlbin, C. (2001). *Information för Marknadsföringsbeslut* (4th ed.). Göteborg: IHM Förlag.
- Li, X., Li, Y., Liu, T., Qiu, J. and Wang, F. (2009). *The Method and Tool of Cost Analysis for Cloud Computing*. In IEEE International Conference on Cloud Computing (CLOUD-II 2009), Bangalore, India, September 2009, 93-100.
- Lublinsky, Boris. (2009, April 22). *Cleaning the air on Cloud Computing*. Retrieved May 08, 2010 from <http://www.infoq.com/news/2009/04/air>
- Lynch, M. (2008) *The Cloud Wars: \$100+ billion at stake*. Merrill Lynch research note, May 2008. Retrieved May 15, 2010 from <http://web2.sys-con.com/node/604936>.
- Mayur, P., Adriana, L., Matei, R., and Simson, G., (2008). *Amazon S3 for Science Grids: a Viable Solution?* In Data-Aware Distributed Computing Workshop (DADC).
- Marshall, C. & Rossman, G.B., (1989), *Designing Qualitative Research*, Newbury Park, California: Sage.
- Preece, J., Rogers, Y. & Sharp, H., (2002). "Interaction Design - Beyond Human-Computer Interaction", John Wiley & Sons.
- Qamar, S., Lal, N., Singh, M., (2010). Internet Ware Cloud Computing: Challenges. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 3, March 2010.
- Rosenthal, A., Mork, P., Li, M., Stanford, J., Koester, D., Reynolds, P., (2009). *Cloud computing: A new business paradigm for biomedical information sharing*. Journal of Biomedical Informatics. Journal homepage: www.elsevier.com/locate/yjbin.
- Rangan, (2008). K. *The Cloud Wars: \$100+ billion at stake*. Tech. rep., Merrill Lynch, May 2008.
- Siegele, (2008). L. *Let It Rise: A Special Report on Corporate IT*. The Economist (October 2008).
- Stake, R. E. (2005). Qualitative case studies. In N. K. Denzin & Y.S. Lincoln (Eds.), *The Sage handbook of qualitative research* (3rd ed.; pp. 443-466). Thousand oaks, CA: Sage.
- Stanoevska-Slabeva, K., Wozniak, T. (2009). *Grid Basics*. In: *Stanoevska-Slabeva, K.,*

Wozniak, T., and Ristol, S., *Grid and Cloud Computing A Business Perspective on Technology and Applications*. Springer Berlin Heidelberg, 2009.

Sullivan, T. (2009). "The ways cloud computing will disrupt IT," http://www.cio.com.au/article/296892/nick_carr_ways_cloud_computing_will_disrupt_it.

Vogels W, (2008). Beyond Server Consolidation. Queue 2008; (p 6:20–26). Available at: <http://portal.acm.org/citation.cfm?id=1348590&coll=Portal&dl=ACM&CFID=78225754&CFTOKEN=19192256&ret=1#Fulltext>.

Weishäupl T., Donno F., Schikuta E., Stockinger H., Wanek H. (2005). *Business In the Grid: The BIG Project*. In: Proceedings of the 2nd International Workshop on Grid Economics and Business Models (GECON 2005). <http://hst.home.cern.ch/hst/publications/gecon-2005-BIGproject.pdf>. Accessed 5th May, 2010.

Window Security, (2010), <http://www.windowsecurity.com/articles/Security-Cloud-Trustworthy-Enough-Your-Business.html>. Retrieved on April 11,2010.

Yin, R. K. (2003): *Case study research: design and methods*. 3rd ed., Sage Publications, California: Thousand Oaks.

Youseff, L., Butrico, M. and Da Silva, D. (2008). *Toward a Unified Ontology of Cloud Computing*. In Grid Computing Environments Workshop (GCE '08), Austin, Texas, USA, November 2008, 1-10.