1-1-2012

An Overview of Cloud Computing Challenges and Its Security Concerns

Krishnun Sansurooah

An Overview of Cloud Computing Challenges and Its Security Concerns.

Krishnun Sansurooah
SECAU Security Research Centre, School of Computer and Security Science
Edith Cowan University, Perth, Western Australia, Australia

Abstract *- There has been an increasing advancement about Cloud computing during the past couple of years. Cloud computing has become a new computer model which aims to deliver reliable, customizable and scalable computing environment for end-users. Companies are choosing to move their data, applications and services to the Cloud. The advantages are significant ranging from increasing the availability, reliability, light weight, easily accessible applications, and low cost but so are the risks associated with. Companies that require application hosting could potentially benefit from the provisioning of computing infrastructure resources as a service. In addition to the economic advantages of an on-demand computing environment, businesses also enjoy the flexibility to scale up or down their services to accommodate the changing nature or the business requirement without having to invest in new equipment however, migrating data to the Cloud exposed the data to be an easy and vulnerable target for all the maliciously intended actors all over the world. This paper brings an introduction overview to Cloud computing, it's enabling technologies behind such a design, its evolution and finally the security concerns that is entails.*

Keywords: Cloud computing, infrastructure models, cloud security

1 Introduction

Cloud computing derives its name from the drawings normally used in the description of the Internet with a new retention and delivery of Information Technology (IT) services. It originated in the late 2007, but currently came forward as an enticing topic due to its abilities to offer and deliver adaptive dynamic IT infrastructures, quality of standards computing environment and softwares services that can be used by businesses having different needs.
The idea of Cloud computing definitely represents a change in the way of addressing things which the end user does not have to fully be knowledgeable of the details of a specific technology. According to Google trends [8], it has been reported that the Cloud computing has overtaken virtualization in popularity as depicted by figure 1 below with the blue line which is sitting above both the virtualization technology in yellow and the red line representing Grid computing [5].

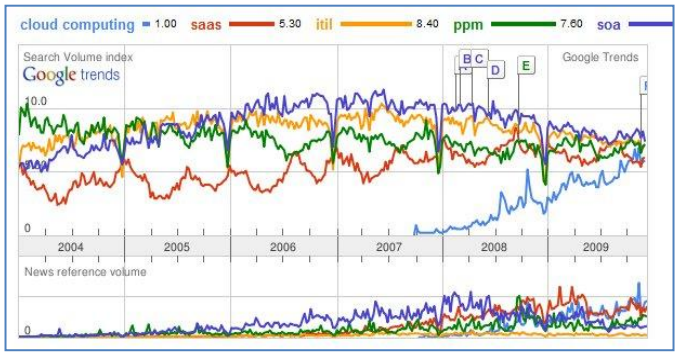

Figure 1. Cloud computing surpassing virtualization in popularity ***(Google Trends, 2009).***

Huge companies such as IBM Blue Cloud [10] and the European Union have joined forces to collaborate on a research programme for Cloud computing, Amazon Elastic Compute Cloud, [2] scientific projects such as Nimbus and Stratus which are a set of open source tools that offer an "Infrastructure-as-a-Service" (IaaS) cloud computing solution. [14].

The term Cloud computing is a common overused computer term that most computer professionals have used as "public internet" at one time or the other. There is still no such universal definition for the Cloud computing despite that Cloud computing practices have characterized much attention in the past years. Many arguments have lead to this setting:

- Cloud computing includes working in collaboration with researches, network engineers, from different experiences and environments;
- The technologies that permits clod computing to exists is still in evolution and progressing;
- Prevailing computing Clouds however comes short of acceptable measure of deployment and usage which would substantiate the conceptualization of Cloud computing.

This paper will consolidate what Cloud computing is using simple and commonly acceptable terms whilst elaborating on the other sections of this paper such as the evolution of Cloud computing, the various Cloud computing infrastructure models, its enabling technologies, what benefits does Cloud computing has to offer and an in-

depth analysis of the security concerns with remedial actions to mitigate the threats that Cloud computing poses.

2 Definition of Cloud Computing

Gradually, businesses of all sizes are choosing to migrate their data, applications and services to the Cloud [6].Cloud computing is becoming one of the next IT trends where IT Administrators, managers and CEO are porting their data and applications to remote "Clouds" and accessing these data in a simple and ubiquitous manner from anywhere around the world. However not much considerations is given due to the vulnerability of the data which becomes a tantalizing target for hackers which will be discussed further in the overview of the security concerns of the Cloud computing. Cloud computing can be generally defined as numerous diverse ways to distribute information or services to customers who pay what they use. Obviously, the customer can either be an individual or a business purchasing for a service or information. Cloud computing is nothing less that a new approach of conducting business that seizes the advantage of housing various competencies into a particular structure that can then extended to host out services for multiple businesses.
Due to the ongoing evolution of the Cloud Computing, it is quite premature to come up with an exact definition of what is Cloud computing? However, at this early stage we believe that the Cloud computing definition could be summaries as:

- *"A range of network enabled services, having the ability to be expanded, quality of standards, usually customizable, with inexpensive computing infrastructure and environment on demand to the availability of the customers that can be accessed easily form anywhere."*

However according to National Institute of standards and Technology (NIST) in 2009, their definition of Cloud computing was defined as:

- *"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This Cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models."*

3 Evolution of Cloud Computing

The growth of Cloud computing can be traced back to the Grid computing. The idea of "The Grid" gained in popularity after Foster and Kesselman [5] published their work *"The Grid: Blueprint for a new Computing Infrastructure"*. It was founded on the electric grid that provides electric power to your home and business. This time it would be oriented towards using the same concept in hardware and software which would be provided from the grid on-demand from a computing level [3].
One of the most interesting downfalls with Cloud computing is that the same issues that hit the grid did the same for Cloud computing which at present still suffers from the formation of standards, whether vendor have to be locked-in, etc.
Cloud computing is about moving services, computation and or data for an inexpensive cost which will benefit the business. It is location-transparent with a centralized facility. By making data available through the Cloud, it can be more easily accessed from everywhere at a much lower cost, increasing its value by allowing favourable circumstances for improved collaboration, integration and analysis on a shared common environment/platform which leads to have various choices of Cloud computing infrastructure models.

3.1 Cloud Computing Infrastructure Models

Prior to migrating the data, applications and services to the Cloud, there are several considerations that need to be taken into account as moving from a standard enterprise application deployment to a Cloud computing architecture could cause the entire business to collapse.
There are public and private Clouds that propose integrative advantages which IT companies can select to extend the use of applications on private, public or hybrid Clouds each of which have their gives-and-takes illustrated in figure 2.

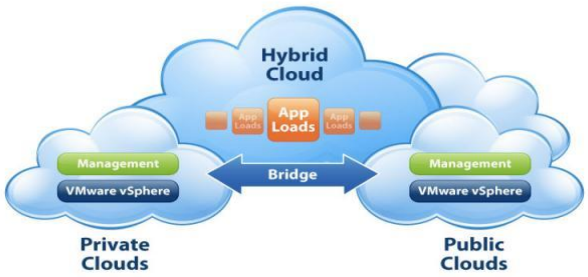

Figure 2. Illustrates the different types of Clouds and their interactions, public, private and hybrids.

3.1.1 Public Clouds

Public Clouds are usually run by third parties; and applications from various clients are probably merged together on the Cloud's server, storage systems and networks as depicted in figure 3. Public Clouds are normally hosted offsite from the client's localities which hence reduces the customers cost and risk by accommodating an adaptive extension to the enterprise infrastructure. It is also to be noted that if the public cloud introduce performance, security and data centralization, the existence of the other applications running on the Cloud will have to be transparent to both the Cloud architect and the end users. In this sense the benefit of public Clouds is that they can be much larger than a company's own private Cloud providing the ability to scale up or down on demand.

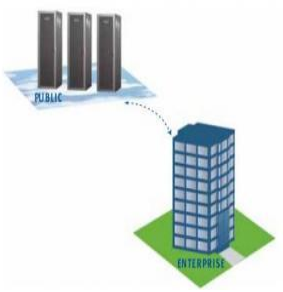

Figure 3 depicts a public Cloud providing services to multiple customers which set up at a collocation facility [13].

3.1.2 Private Clouds

Private clouds are built for the exclusive use of one customer, accommodating the absolute control over data, security, and quality of service as depicted in figure 4. The company is the owner of the infrastructure and has got total control over how applications are set up on it. Private clouds can either be built in an enterprise data centre or they can also be deployed at a shared facility.

Private Clouds can be put together and controlled by a business own IT department or by a Cloud provider. In this model a company can install, configure, and operate the infrastructure to support a private Cloud within a company's enterprise data centre. This infrastructure allows businesses with an utmost level of control over the use of Cloud resources while accommodating the necessary expertise to settle and manage the environment.

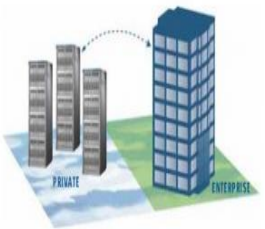

Figure 4 shows how Private Clouds may be hosted at a collocation facility or in an enterprise data centre. They may be supported by the company, by a Cloud provider, or by a third party such as an outsourcing firm.

3.1.3 Hybrid Clouds

Hybrid Clouds as it name say it all it is a combination of both public and private Cloud models as shown in figure 5. These Clouds assist with on-demand and externally provisioned scale. The ability to improve a private Cloud with the benefits of a public Cloud can be applied to preserve the service levels in the case of quick evolving workload variations. This is visible in making use of storage Clouds to assist Web 2.0 applications for example. Hybrid Clouds brought forward the intricacies of deciding how to allocate the applications across both a public and private Cloud. Among the different concerns that needed to be taken into account is the connection between data and processing resources. If the data is small and of not major importance, or the application is in a stateless condition, a hybrid Cloud would have more success rather than transferring a large amounts of data into a public Cloud for a small amount of data processing.

Figure 5 shows a Hybrid Clouds combine both public and private Cloud models, and they can be particularly effective when both types of Cloud are located in the same facility.

3.2 Architectural Layers of Cloud Computing

Ideally, users access computing platforms or IT resources from Cloud computing and then run their applications from the inside. Therefore, Cloud computing provide the users with services to access hardware, software, platform based, infrastructure and finally data resources, thereafter an integrated computing environment as a service in a evident way as illustrated in figure 6.

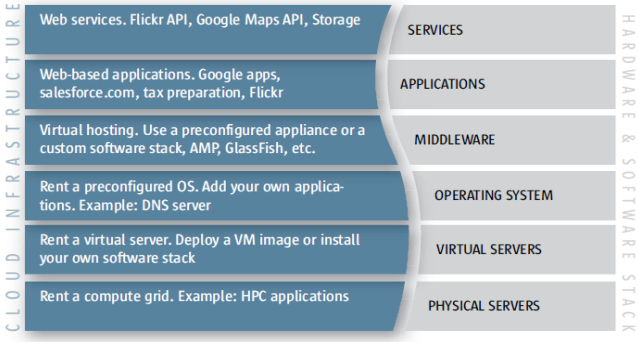

Figure 6 depicts Cloud computing as one that can provide services at various layers from hardware to applications.

3.2.1 Hardware as a Service (HaaS).

As a result of technology advancing rapidly, hardware virtualization has done the same hence allowing businesses to buy IT hardware, if not, a whole data centre, as a pay-as-you-go subscription facility [16]. The HaaS is flexible, scalable and manageable to meet your needs.

3.2.2 Software as a Service (SaaS).

This model is designed to be hosted as a service and provided to customers across the Internet. In a nutshell this model provides everything and simply rent out the software to the user through some sort of front end or web portal thus eliminating the burden of installing and running the application on the client's local machines. A single instance of the software runs on the Cloud and services multiple end users or client organizations. Another advantage of this SaaS is that it relieves the client's burden of software maintenance and reduces the expense of software purchases by on-demand pricing.

3.2.3 Platform as a Service (PaaS).

With this particular approach of Cloud computing, PaaS as a service covers a panel of software and delivers it as a service that can be adopted to develop or build higher-level services. This can be categorized into 2 groups. Firstly, PaaS, provides a platform for working while combining an operating systems, application software and a development environment that is then put at the disposition of the client as a service and secondly, as a customer making use of the PaaS as a service would see a tremendous advantage in a wrapped service that is proposed to them. Since PaaS model of Cloud computing includes all phases of the System Development Life Cycle (SDLC), the customers could interact with the platform through an application program interface (APIs), website portals or gateway software.

3.2.4 Infrastructure as a Service (IaaS).

This model encapsulates the delivery of basic storage and calculates competencies as standardized services over the network. As the name implies, the customer is buying the infrastructure. Servers, storage systems, switch, etc... are made available to administer workloads from computing application.

3.2.5 Data as a Service (DaaS).

Data in numerous formats and from different sources could be accessed through the services by customers on the network. User could therefore alter the remote data just like performing data changes on a local disk or accessing data in an acceptable manner. Therefore, the user pays only for the storage capacity that they require and the bandwidth for that particular storage. However the system is flexible and scalable as it allows businesses to add capacity as needed, in-demand.

4 Technologies Behind Cloud Computing

There are various enabling technologies that contributes to the successful achievement of Cloud computing. These precursors are identified as:

Service Oriented Architecture (SOA)

It is essentially a collection of services which communicate with each other by either simple data passing or it could involve two or more services organizing some activities. Since computing Clouds are normally opened to work with Web Services such as WSDL, SOAP and UDDI, the services provided by the SOA could be used to orchestrate and organize these services. Furthermore, a set of Cloud services could be used in a SOA application environment thus taking advantage of having them available of multiple distributed platforms accessed through the Internet.

Virtualization technology.

Virtualization is software technology which uses a physical resource such as a server and divides it up into virtual resources called virtual machines (VM's) which offers virtualized IT infrastructures on-demand. Virtualization permits users to strengthen physical resources, simplify arrangement and administration whilst abating power and cooling requirements. While virtualization technology is most popular in the server world, virtualization technology is also being used in data storage such as Storage Area Networks, and inside of operating systems. Virtual networks such as Virtual Private Networks (VPNs) assist users with customized network environments to access Cloud resources as they are the foundations of Cloud computing as they depict flexible and scalable hardware resources.

Inexpensive Worldwide Distributed Storage.

A network storage system which is supported by distributed storage providers also known as data centres (sometimes called server farm) which are at the disposition of the users for loan. Therefore, the need of having a centralized repository for the storage, management and dissemination of data and information. One key advantage of the data centre storage concept is that physical hard drive storage resources are combined into a collection of storage pools. Another benefit that contribute to the use of Cloud computing is the consolidation of all facilities encapsulating HVAC, electrical, network connections, wiring, hardware, software and personal. Hence a distributed data system which can support data sources to be accessed in a ubiquitous manner.

Web 2.0
Web 2.0 is a new technology which apparently helps in distinguishing the use of the World Wide Web technology and Web design pertaining to the creativity, information sharing, and collaboration to the Web. The main idea behind Web 2.0 is to uplift the interconnectivity and the interactivity of the Web applications enabling users to access the web more easily and efficiently. And since Cloud computing resources are based on web applications, it makes it natural that while evolving, Cloud computing will favour the use of Web 2.0.

Service flow and workflow.
Cloud computing provide an entire set of service templates on-demand, which could be comprised of services from the inside Cloud. Therefore, the Cloud should be able to naturally if not automatically coordinate services from various sources to form a flow of service which is transparent and dynamical to the users.

4.1 Benefits of Cloud Computing.

The primary aim of Cloud computing is to decrease the cost for computing resources whilst leaving if not increasing the flexibility and scalability of the system. This model also minimizes capital expenditures, since the concept of renting out the services from a different provider on a peruse fee the business only pays for the used resources. The sharing of resources and purchasing power of very large scale, data centres provides economic advantages are listed below:

- ***Reducing high fixed-capital cost to low variable expense***
  Creating an internal cloud within a company supports an efficient service platform while monitoring internal capital consumptions for the IT infrastructure. This could then be exploited with an external cloud service provider that could jump on board to supply overflow service capacity when demand increases above the internal capacity.
- ***Flexibility***
  As with large businesses, the ease of deploying a full service without having to organize the base environment to support it can be even more attractive that cost savings. There is the ability to update the hardware and software quickly to comply and suit customers' demands and updates in technology.
- ***Smoother scalability path.***
  Cloud computing allows for many singles services to scale over a wide demand range. It multiplies resources load balance peak load capacity and utilization across multiple hardware platforms in numerous locations.
- ***Drastically reduces cost (Disaster Recovery).***
  Especially with small to medium enterprises, make no investment in disaster recovery (DR) plans. But with enabling technologies such as the virtualization – VMWares (virtual machines) to be transferred to the Cloud for access whenever it is needed, it has evolved in a cost effective disaster recovery model since the DR plans cost twice the infrastructure whereas with a Cloud computing approach the DR is available for much cheaper hence making a significant difference in cost for the businesses.
- ***Self-service IT infrastructure.***
  Cloud computing service models are often self-service, even in internal models. As before the business had to partner with the IT to develop your applications, port it onto a platform and run it but with Cloud computing all this is not of the past. You are purchasing infrastructure.
- ***Increased automation and portability***
  Moving into the Cloud computing requires a much higher level of automation because moving off-premises terminates on-call systems administrators. It also increases the portability of the system whereby users can work from home, work or at client location thus increasing mobility that employee can access information anywhere they are.
- ***Centralization.***
  Centralization of critical data improves security by eliminating data from user's computer. Cloud computing providers have the necessary knowledge and resources to provide all the latest security features to guard the data.
- ***Maintenance.***
  With centralized applications, they are much easier to maintain than their distributed counterparts. All updates and changes are made in one centralized server rather that on each user's computer.

4.2 Security Concerns of Cloud Computing.

While cost and ease of use are among the great advantages of Cloud computing, there are alarming security concerns that need to be taken into consideration when being inclined to move critical applications and especially sensitive data to public, private or hybrid Cloud environments. To focus on these issues, the cloud provider must implement and develop acceptable measures to match the same if not extended layers of security than if the business would have if they were not to use the cloud. Listed below are the main concerns that should be taken into consideration prior to porting all their sensitive data and applications to the remote "Clouds" as these can very quickly become appealing targets for people of criminal intentions. Below is an overview of these issues that have been summarized into three different categories that should be thought prior to change to the Cloud computing infrastructure.

Conventional Security: These issues would be involving computer and networks intrusions or attacks which could have a potential of occurring since moving to the cloud.

i) **Authentication and Authorization**: the company's authentication and authorization structure does not extend into the cloud which if it does can cause problems with the cloud provider's schema provided that the cloud provider has got one in place. According to Jericho Forum (2010), it would be easier to lock and protect information if it's managed by a third party than it was in-house. So the question here is how the organization remodels its existing structure to accommodate the cloud computing infrastructure model. Furthermore, how does an organization combine cloud security within its own security policies?

ii) **Phishing:** What are the countermeasures that are set up to reduce the risks of being hit with phishing scams which have new attack vectors?

iii) **Virtual Machine attacks**: Potential attacks lies within the virtualization area – i.e. VM technology used by cloud vendors hence the introduction use of firewalls and intrusion detection systems should be part of the system to monitor system activities.

iv) **Network attacks**: The cloud user should ensure that the infrastructure used to connect and interact with the cloud is protected at all times which could be a gigantic task as the cloud is designed and set up outside the firewall in most of the cases.

v) **Forensics implications:** At present, the conventional methods of digitally forensically analysing equipment is to seize the devices and image them and perform an in-depth analysis of the media and then recover the data from. But with cloud computing the likelihood of conducting forensics analysis would be very complicated to perform due to the nature providers maintaining their own multi-server infrastructure and hence data being overwritten multiple times.

Availability of data: Based on critical applications and data being made available for the users to access anytime and from anywhere around the globe.

i) **Uptime:** most cloud providers dispute the fact that their server uptime is with reasonable parameters compared to the availability of the cloud users' own distributed centres.

ii) **Single point of failure:** Cloud computing services are meant to provide more availability which is not the case but instead are open to more single points of failure.

iii) **Computational integrity:** Can an organization guarantee that the cloud provider is being trustworthy and faithful in running hosted applications and resources which are feeding back trustworthy outcomes for the smooth running of the organization.

Data-control by external parties: What are the legal ramifications and implications of data an applications being under the control of external parties? Because this area is not well understood and very complex, there are potential lack of control and transparency when a third party is involved in the process of containing all the data.

i) **Audit ability**: Is another issue of lack of control in the cloud which then bring up the question is there enough transparency in the way of conducting operations from the cloud provider's side? This is very important as it hence build up the trust between both the provider and the user.

ii) **Contractual Obligations:** One of the various issues that emerge when using a third party infrastructure is the legal implications. Hence the implementation of service level agreement (SLA) or what can and what cannot be done bounded by a written contract.

iii) **Data loss or leakage: T**here a numerous ways of compromising the data. Modification, fabrication, deletion of data without a proper backup of the original or updated data is a very common example. Loss of encryption key could lead to data not being disposed properly. The threat of compromising data is multiplied on the cloud due to the numerous interactions of users with the environment is dangerous due to the architectural design of the cloud environment.

iv) **Data lock-in:** How does a cloud user abstain from locking-in to a particular cloud vendor? Also there is the problem that the cloud users have no control over the regular changes that the cloud provider is effecting from his side.

5 Remedial Strategies for Addressing Cloud Computing Risks

The risks that an enterprise might recognize must be dealt with in an effective manner. A robust risk management program that is flexible enough to deal with continuously evolving information risks should be in place. In an environment where privacy has become the utmost priority to enterprise customers, unauthorized access to data in the cloud is of major concern. When agreeing to a service level agreement (SLA) with a cloud provider, the organization (user) should imperatively record all his information assets.

The organization should also make sure that data are correctly catalogued. This process should be implemented while drafting the SLA which will determine a legally contract between both the user and the provider. Any specific needs of the user such as data need to be encrypted before being transferred or transiting or stored from one location to the other, and additional controls for information that is sensitive or of high value to the organization should be clearly defined in the agreement.

The SLA is a legal document that characterizes the relationship between the business and the cloud provider, it also serves as a powerful tool to protect against information entrusted to the cloud. Listed below are some of the remedial actions that should be implemented when considering cloud computing environment:

- ***Abuse use of Cloud computing***
  - i) Effectively analysis of user network traffic whilst monitoring public blacklisted network blocks
  - ii) Tighter initial registration and validation process when it comes to using credit card. (everyone can use a credit card to purchase and immediately start using the cloud services)
- ***Insecure Application Program Interfaces***
  - i) Scrutinize the security model of the cloud providers
  - ii) Making sure that strong authentication and authorisation is implemented with encrypted transmission.
- ***Threats from insiders***
  - i) Making sure that there is a reliable security breach notification in place.
  - ii) Requesting transparency in information security practices as well as compliance reporting
  - iii) Including human resource requirements as part of legal contracts
- ***Shared technology***
  - i) Monitor for unauthorized activities.
  - ii) Conduct vulnerability scanning, configuration auditing while ensuring that SLA mentioned the patching and upgrading of the environment
  - iii) Promoting strong use of authentication and access controls for any levels of operations.
- ***Data Loss or leakage***
  - i) Implementation of strong encryption to protect integrity of data in transmission
  - ii) Ensure that strong key generation, storage and management and destruction policies are in place
  - iii) Analyse and monitor data protection on both ends.
  - iv) Prohibit the sharing of account credentials between users and resources
  - v) Use strong 2-way authentication wherever it is possible.
  - vi) Understand cloud provider security policies and SLAs.

6 CONCLUSION

Cloud computing proposes valid advantages to businesses striving for competitive benefits. Many more providers are spreading into the concept of providing Cloud computing services and are therefore driving the competition to a higher level with even lower prices which is an absolute benefit for businesses. Since the Cloud computing provides appealing pricing, the ability to remodel the human resources towards other tasks, the ability to pay for services when needed will drive more businesses to adopt the Cloud computing infrastructure. But before any services are moved to cloud, the business managers should confirm that these actions are rational for the good running of the business. In this paper as we have seen there are the pros and cons of Cloud computing which need to be weighed carefully before any decisions to be made.

7 REFERENCES

[1] ACIS (2001) Status Project. Retrieved 9 August, 2010 from http://www.acis.ufl.edu/vws

[2] Amazon Elastic Compute Cloud (2007). Amazon Elastic Compute Cloud. Retrieved 24, July, 2010 from http://aws.amazon.com/ec2/

[3] Baca, S. (2010). Cloud Computing: What It Is and What It Can Do for You. Retrieved 27 June , 2010 from http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_VI_CloudComputing.pdf

[4] Craig Balding (2008). Assessing the Security Benefits of Cloud Computing. Retrieved 5 September, 2010 from http://cloudsecurity.org/blog/2008/07/21/assessing-the-security-benefits-of-cloud-computing.html

[5] Foster, I. & Kesselman.C (1998). *The Grid: blueprint for a new computing infrastructure*. Morgan Kaufmann

[6] FIERCIO (2009). Securing the cloud: Designing Security for a new Age. Retrieved 28 June, 2010 from http://i.zdnet.com/whitepapers/eflorida_Securing_Cloud_Designing_Security_New_Age.pdf

[7] Global Cloud computing test bed (n.d.). Global Cloud Computing Research Test Bed. Retrieved 21 May 2010 from http://www.hp.com/hpinfo/newsroom/press/2008/080729xa.html/

[8] Google Trends (n.d). Cloud Computing Surpasses Virtualization in Popularity Retrieved 02, August, 2010 from http://www.elasticvapor.com/2009/04/google-trends-cloud-computing-surpasses.html

[9] Here comes HaaS (2006). Here comes HaaS. Retrieved 14 May, 2010 from http://www.roughtype.com/archives/2006/03/here comes haas.php/

[10] IBM Blue (n.d) Cloud Initiative Advances Enterprise Cloud Computing. Retrieved 15, June , 2010 from http://www-03.ibm.com/press/us/en/pressrelease/26642.wss

[11] IBM (2009). Architectural manifesto: An introduction to the possibilities (and risks) of cloud computing. Retrieved 11 May, 2010 from http://www.ibm.com/developerworks/architecture/library/ar-archman10/index.html?S_TACT=105AGX20&S_CMP=EDU

[12] Mell, P & Grance T. (2009). The NIST Definition of Cloud Computing. Retrieved 21, July, 2010 from http://csrc.nist.gov/groups/SNS/cloud-computing/

[13] Sun's View (2009). Overview of Cloud Computing. Retrieved 29, July , 2010 from http://hiencs.wordpress.com/2009/09/01/overvire-cloud-computing-architecture/

[14] Nimbus (2010) Nimbus Project. Retrieved 10 July, 2010 from http://workspace.globus.org/clouds/nimbus.html/
Understanding Cloud Computing (2009). A white paper for executives making decisions on computing resources. Retrieved 19, July, 2010 from https://ritdml.rit.edu/bitstream/handle/1850/7821/LWangConfProc11-162008.pdf;jsessionid=4D6164F12ABFD986C5891A8762A9B4A9?sequence=1

[15] Understanding Data Centers and Cloud Computing from http://images.globalknowledge.com/wwwimages/whitepaperpdf/WP_DC_DataCenterCloudComputing1.pdf

[16] Wang & Laszewski. (2008)Cloud Computing: a Perspective Study. Retrieved 20, August, 2010 from https://ritdml.rit.edu/bitstream/handle/1850/7821/LWangConfProc11-16-2008.pdf;jsessionid=4D6164F12ABFD986C5891A8762A9B4A9?sequence=1

[17] The Jericho Forum's demolition framework (2008). Don't Cloud Your Vision. Retrieved 4 August, 2010 from http://www.ft.com/cms/s/0/303680a6-bf51-11dd-ae63-0000779fd18c.html?nclick_check=1

[18] Trapani, G (n.d). The Hidden risks of cloud computing. Retrieved 15 August, 2010 from http://lifehacker.com/5325169/the-hidden-risks-of-cloud-computing