Cloud Computing Security Issues

MSc in Software Engineering at DE Montfort university
Entsar Alahwal (ent20022003@yahoo.com)

Abstract

In the last three decades, the concept of computation has changed from centralized (client-server not web-based) to distributed systems and recently users are coming to the Cloud Computing "virtual centralization". Cloud computing is where data, software applications, computer processing power, can be accessed from cloud on line resources. On the one hand, an individual user can access data and applications from any device connected to the internet. What is more, data maintenance and the service is provided by the vendor which means the customer/client is unaware of where the data is, what processes are running or where the data is stored. So, logically, the customer/client has no ability to control over it. The internet is fundamental as the communication media of the cloud computing. This poses a substantial security concern for cloud computing. Guaranteeing the security of data is difficult as they provide numerous services such as Virtualisation, Utility computing, Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS) Each of these services have their own issues of security, the vendor of cloud computing has to provide some guarantee in service level agreements (SLA) to convince the client that security issues have been considered and measures have been taken to ensure an adequate degree of security. The SLA has to illustrate diverse levels of security based on the various services to allow the client to understand the policies of the security which are being implemented. This project identifies issues related to cloud computing that should be considered by security practitioners. Three types of cloud computing issues are examined: integrity, availability, and confidentiality, and inspect the techniques that can be employed to counter them.

KEYWORDS cloud computing , security, issues IaaS, SaaS, PaaS, availability, integrity, and confidentiality.

1. Introduction

There are diverse types of computing that led to the development of Cloud Computing. Grid Computing in the early 1990's was famous as the peer-to-peer networking; allowing virtual computers to structure a network to achieve very large tasks [100]. Subsequent Grid Computing, Utility Computing started in 1961. This idea died after a couple of years was then brought back in 1998 by Hewlett Packard. The idea of an "intergalactic computer network" was proposed by J.C.R. Licklider, who was responsible for the improvement of Advanced Research Projects Agency Network (ARPANET) in 1969. His vision was everybody in the world to be interconnected and be able to access data and programs from anywhere at any location.

Utility Computing is known as an on demand service, where customers access their own data via the internet or private lines. Some say Utility Computing developed into "Cloud Computing".[101] The Autonomic Computing is a new term which came before "Cloud Computing". The word "Cloud" of Cloud Computing represents the internet. The Cloud is the network joined with the computing infrastructure.

2.1What is cloud computing?

Cloud computing is the next stage of development of on-demand information technology services, cloud computing based on virtualized resources. It provides different services which are based on different capabilities services such as Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS), Virtualisation, grid and Utility computing. The definition of cloud has been discussed by 20 different authors; definitions of cloud computing are as follows:

"Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLA" [14].

According to National Institute of Standards and Technology (NIST), cloud computing is a model used for enabling suitable, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications, and services) which can be quickly provisioned and released through service provider interaction or minimal management effort. This cloud model encourages availability and is collected for essential characteristics, models deployment, and various service models [15].

Cloud computing indicates a rising model of computing where data in large machine centres can be dynamically provisioned. These are configured and reconfigured to distribute services in scalable methods, for wide requests from scientific research to e-mail to video sharing [16]. It is usually expressed as a single entity although cloud computing can includes numerous components at once: cloud applications, cloud platform, cloud infrastructure and the provision of cloud infrastructure as a service, both storage and resource are components such as Amazon's Elastic (EC2) and S3 service [17]. This infrastructure allows clients to construct the infrastructure themselves, in addition to containing the rapid expansion of their infrastructure, which is based on network requirements. A Cloud platform is the provision of software stack or a computer platform as a service, such as salesforce.com or Google's App engine. A Cloud application is web services that run on an upper level over a cloud infrastructure or platform which is available to the customers or organization's users. They can contain applications which are more popular such as Google Docs as a set of office applications, and video on YouTube's as hosting applications.

Providers of Cloud offer different services to individuals, corporations, small or big companies and government agencies. Cloud computing is used for clients employing sharing and storing of information, and database management. In addition, deploying Web services can range from processing huge databases, for complex scientific problems, and to use cloud to manage and offer access to medical records [7]. The incredible processing capacity level of data and information which is available in the cloud the petabyte scale allows new approaches to analysis data [18]. Clients may use cloud computing to store their documents and e-mail. Large groups of scientists and companies can use the huge computing power which is available to insert another dimension to their recent IT infrastructure [16].

Cloud computing opens up the opportunity of a main cloud provider such as Google so that they could finally become the world's primary computer [19]. Cloud computing speaks for a computing resource and centralization of information - quite opposite to the images that address evokes, and several, individuals, companies, and government agencies are already frequent or constant users. Already unknowing clients are taking benefit of the cloud throughout Web-based on-line data storage service and software applications, such as YouTube, Flicker, and Google [20].

The conception of cloud computing is not only to change the infrastructure of organizations, but also how they do business. As federal CIO Vivek Kundra has stated, ".....it's a fundamental change to the way our government operates" [16]. Accordingly, the government of federal has already started to apply cloud computing in their IT strategies [21]. In addition, the Obama Administration has interest in the large –scale use of cloud computing for processing and government storage [22]

This focus going on the electronic provision of information via the Obama Administration would take the government closer to the social expectations of several citizens. Now the majority government of information is digital, and clients want to access it electronically [23]. A 2008 study found 77.4% of users seeking services or government information regularly by using Google or any commercial search appliance [24]. Although, providing ever rising amounts of communication, government information, and services on-line increases serious issues about equality between people with limitation of technological means to contact e-Government [25].

According to Dikaiakos, the vision of 21st century is accessing the services of internet by light weight portable devices, instead of accessing it by a traditional Desktop PC. Cloud computing as technology has allowed individual users, companies or organisations or any enterprise to host their services without worrying about supporting services and IT infrastructure. Cloud computing comes from existing technologies which are not new such as Distributed Computing, Centralised Computing, Utility Computing. On the other hand what is new is that it integrates all the above to move them from a processing unit to virtualisation centre [26], [27].

The facilities of cloud computing start at a company by moving Capital to Operational Expense [29]. Amazon (EC2,S3),Google App, IBM Blue Cloud, HD Cloud Assure, Microsoft Azure, all of these services are available in the market of cloud computing [28].

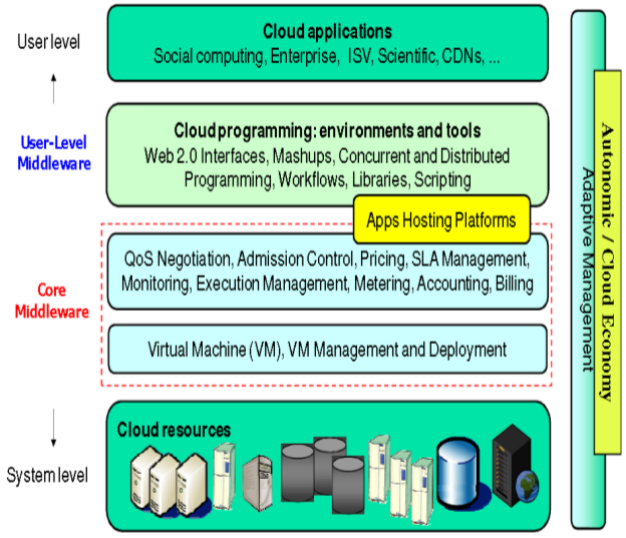
2.2 Why is it significant?

Cloud computing offers IT organizations with a diverse model of operation; many advantages of cloud such as the maturity of networks, web applications, and the increasing interoperability to provide IT services of computing systems. Cloud provides particular services and applications and this expertise allows them to manage maintenance, backups, disaster recovery, upgrades, and failover functions. As a result, customers of cloud services can see the rising of reliability, even as costs rise due to economies of scale or other factors. With cloud computing, companies can observe current needs and make modifications of capacity to increase or decrease, find spikes in demand to avoid paying for unused capacity through slower times. Beside the potential of lower costs, universities and colleges gain the flexibility of quick response to requests for new services when purchasing them via the cloud. Cloud computing encourages and provides IT organizations to increase standardization of processes and protocols. So that the many parts of the cloud computing model can be efficient and interoperate. Another key benefit of cloud computing is scalability for higher education, especially for research projects which require vast amounts of processing capacity and storage for a limited time. Some organisations have built data centres close to sources of renewable energy, such as hydroelectric facilities and wind farms, cloud computing affords access to these providers of "green IT." Finally, cloud computing allows university and college IT providers to make the costs of IT apparent. So IT services consumption can be matched to those who pay for such these services.[30]

2.3 Cloud Computing Architecture

Figure (1) shows the design of a service-oriented layer of Cloud computing architecture. Core middleware capabilities with physical Cloud resources form the foundation for delivering IaaS. The aims of the user-level middleware layer provides PaaS capabilities. The top layer User level focuses on application services (SaaS) via making use of services provided through the lower layer services. PaaS/SaaS services are provided and developed often by 3rd party service providers [34].

2.3.1 User-Level Middleware: This layer contains Web 2.0 Interfaces (IBM Workplace, Ajax) as software frameworks which help developers to create rich, cost effective browser user interfaces on which are based applications. Also the layer provides composition tools and programming environments which help applications in the creation, deployment, and execution in Clouds.



Resource : [98]

Figure (1) Layered Cloud Computing Architecture

2.3.2 Core Middleware: The platform level services implemented by this layer provide a runtime environment allowing capabilities of cloud computing to application services built by using User-Level Middlewares. Core services at this layer consist of Billing, Accounting, Dynamic SLA Management, management, Pricing and Execution monitoring. The services operating at this layer are those such as Google App Engine, Amazon EC2, and Aneka [31].

2.3.3 System Level: The computing power is installed with hundreds to thousands of servers in Cloud computing [33].There are huge physical resources (application servers and storage servers) which power the centres of data at the System Level layer. These servers are clearly managed via the higher level virtualization [32] toolkits and services that allow sharing of their capacity between servers virtual instances. These VMs are isolated from another that leads to achieving fault tolerant behaviour, and the isolated security context environments is supplied by a group of data centres[35]

2.4 Cloud computing security issues

What are the security issues that are preventing companies from taking benefit of the cloud? Several studies, for example IDC's 2008 Cloud Services User Survey [43] of IT management, mention security as one of many challenge of cloud users.

This section contains three security issues. The Cloud Security Alliance's initial report [45] includes a different type of taxonomy based on 15 diverse security domains .The main three concerns of the security are:

- Availability
- Confidentiality
- Integrity

2.4.1 Availability

Availability refers to ensuring the information processing resources, unavailability may occur as a result of malicious action. A key importing point of cloud computing is for the client to have 100% uninterrupted availability. For large vendors, maintaining 24/7 up time is essential to their business, as consumers need this amount to enhance their missions significant efforts. However, outages of companies probably occur, and can be costly for the customer [82].

In a recent research of California University, Berkley followed the availability of several vendors of cloud and recorded about four major outages throughout the first four months in 2008. The reasons of these outages are due to overloads on the systems that leads the system to fail. In fact the issue in these cases refers to the vendor of cloud being a single provider, thus a single failure leads the company to failure [46], and the customers of cloud were unconcerned or unaware that the vendor had no back-up or redundancy mechanisms in place. During a period no more than 60 days, Apple Mobile Me, Amazon S3, Citrix, and Google Gmail, all reported periods or outages of unavailability between 2 to 14 h; in March 2009, and about 22 h were losing of Microsoft Windows Azure [47]. The estimated value of market $100 billion by 2011 [48], the outage cost of these companies can reach millions of dollars, without mention of another costs which are caused by lacking confidence via these organizations associates and own customers.

Natural disasters and unexpected events can affect the services of cloud and cause it to be become unavailable. For instance, in June 2009, one lightning strike on data centers of Amazon.com EC2 caused the loss of the service of cloud about 4 h. This was the third time in the last 2 years, and was a wide-spread outage [49]. On the other hand the vendor of cloud should be able to compute the demand from its services, in fact, this calculation based on the Request or its customers' services. This incorrect science has the potential of error which can lead to over capacity of cloud. Once the capacity of cloud reaches greater than 80%, cloud servers and local computers will "thrash" via constantly exchanging data among disks and computer memory. This leads computers to become unresponsive. If the design of the cloud is lacking enough slack resources to control a situation where over capacity happens, the whole cloud can fail [50]. The control to reduce this risk "is that when clouds reach their capacity limit, they could be architected so that applications can request no more computing capacity. They could gracefully degrade each application's usage, which

could prohibit the application from working, but allow the cloud itself to remain functional". [82], [105].

Any outage based throughout overcapacity will have costs (both reputation and financial) to the client. For assessing bids of cloud services, the specialists federal procurement would need a deep understanding of the impacts and risks of even a minute's outage and what would be an acceptable range of downtime on a site-wide basis before a contract be awarded. Another risk of availability is how the priority of customers on the cloud is determined should the entry of overcapacity be reached. If the capacity starts to approach the 80% threshold and confronting some performance or services is necessary, the vendor will be protecting their own services and pass the poverty service to their clients. This risk refers to the need of the client to understand the cloud capacity and how their account will be managed. It is not easy, as a capacity of cloud's reserve is not clear, and data are not public by major cloud providers for competitive reasons. One pointer may be the usage of electrics via a vendor which t is one indication of the amount of technology used in their cloud. [51]. Variability in performance plays a risk to the users of cloud, as they will request a service which is predictable and reliable which will meet their service level requirements .
As cloud computing becomes major, corporations and popular and management entities become clients, that will naturally lead to the services becoming goals of malicious attacks via hackers. Cloud vendors will need to understand the issues which are presented by those. The vendors who can gather a number of complicated services to rejection attacks [52]; this risk was comprehended currently via Twitter and Face book [53]. Dependence on these outsourced vendors could have resulted in a major disconnection of communication inside, across, and with federal agencies. So the impact of this outage of federal users until now is not assessed. Another regard is the availability of the cloud vendor itself. If the vendor is subsumed via another vendor or goes out of business, the availability, safety, and custody of the data it had stored might be in question. In 2008, The Linkup of the cloud vendor rudely ceased operations with notice to its 20,000 clients. According to CEO Steve Iverson, "at least 55% of the data was safe. [54].

2.4.2 Confidentiality

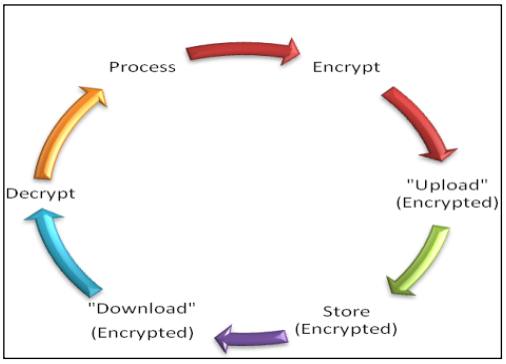
The main aim is to preserve the confidentiality of the database on the cloud. When confidentiality is achieved the entire cell is protected. The definition of a cell's confidentiality is:

DEFINITION1: The confidentiality of a cell is to maintain when no user that does not have access to the cell is able to decrypt it.

DEFINITION2: The scope of a key is the number of cells in the database that the key can decrypt. A user may receive multiple keys to decrypt all her cells. Then her scope is the sum of all her keys. [55].

Confidentiality: refers to ensuring that information is not disclosed to unauthorized persons. Typically, the handle of confidentiality is through the usage of technologies such as access Control and Encryption. It still can be encrypted, but what happens for a large data set? This data has to be assembled or sent in the Cloud.

Thus the data must be decrypted, complete the operations required, and then re-encrypt the



Resource [36]

Figure (5): Lifecycle of Encrypted Data

data and resend to the Cloud. Any data left unencrypted at any stage in the transfer process or in the storage discloses it to unauthorized discovery. Unauthorized disclosure is the reverse of any compliance requirements or good security, such as HIPAA or PCI.

Security indicates confidentiality, integrity and availability, which create major issues of cloud vendors. Confidentiality indicates to who stores the encryption keys data from company A, to company B which stored in an encrypted format, that must be kept secure from unauthorized persons of B; therefore, the customer company must own the encryption keys.

John Krautheim researcher from the University of Maryland [57], also mentions the security and confidentiality issue about Cloud Computing. Krautheim designed the Infrastructure of Private Virtual of cloud security. So users require security over their information, and providers need more security of their own server over the fabric. The level of agreement among the client and provider is very important, because both of them are providing the responsibilities of each party. To observe the security of these parties Krautheim created LoBots.[56] This server provides a continual observing of the cloud communicates and environment to the PVI factory that allowed them to be aware of special situations. (PVI) through this service Krautheim wished to increase security while lowering the cost of ownership of IT infrastructure.

2.4.3 Integrity

Integrity of the cloud infrastructure is ensured through the use of Trusted Computing. In addition, we advocate the seamless extension of control from the enterprise into the cloud through the powerful combination of high-assurance remote server integrity, and cryptographic protocols supporting computation on cipher text. With this approach, content is protected in a manner consistent with policies,

whether in the enterprise or the cloud. Yet, because the protection mechanisms support computation, it is possible for all cloud participants to mutually benefit from the cloud data in a controlled manner. Hence, there is business intelligence advantages derived from operating in the cloud that simply don't exist otherwise. The ability to get smarter through use of the cloud is the key differentiator that will sufficiently alleviate privacy fears to ensure widespread adoption [105].

Integrity refers to all data received and should only be sent or modified by "legitimate" senders, it contains a number of fields that are critical to avoidance or mitigating the risks which affect the accuracy of information managed. Data quality, data validity, and security, speak to the system's operations; integrity is difficult to assess the validity of second generation of data. The processes and decisions involved in deciding which vendor to use and how the system is managed are equally relevant. It also addresses cost and schedule management, as well as performance and program efficacy. All of these are always a challenge for contract management processes and federal acquisitions.

Any information housed via a cloud infrastructure must maintain its accuracy, its integrity with the context to be of value to the client. The provider of cloud must ensure that all protections are taken to guarantee that data in the cloud storage has not been changed or corrupted; this will be not a safe assumption without a defined SLA. Recently, a provider of cell phone which stored data of customers (such as, contact lists, personal text messages, etc.) the provided cloud in a Microsoft subsidiary became unavailable when the provider missing that data. Clients wait days to be informed of that risk, with no guarantee that data might be restored. Although, there is the level of data integrity, the timeline to restore, and the extent of data recovery [58] and the question of responsibility and liability appears. If the problem occurs, who would be responsible or liable for the problem, remediation and ensuing results? Could responsibility be determined based on the infrastructure? Without detailed knowledge of SLAs, these issues will not be easy for both government and the vendor to resolve. Due to a lack of law of challenging case and federal policy, who owns information once it is remanded to a cloud's care is not apparent. For instance, if a federal or soldier employee posts to a federal blog housed in a cloud, the terms of service among the cloud and the agency would decide who owns and controls their information. If the user is unaware of those terms and that information is breach, who would suppose that liability? This shows interesting implications of the double edged of sword that is the balance among free expression, verifiability, information accuracy, and accountability. All of these lead to threat of government although outsourcing such as IT technology. When outsourcing happens, it will become very important that the contract language reflect the needs and requirements of this language and is focused on the agreement of service level which include details measurements of performance and standards [59]. To provide assurance on the privacy and security for both services and data must integrate the requirements of the government's risk management plan.

Conclusion

In conclusion of this paper, it is apparent that the cloud computing security itself is in evolving stage and the security implications are not complete. Still the leaders of cloud computing security providers such as Google, Amazon,etc are facing many security issues and are yet to stabilise. To achieve complete solution for legal issues is still an unsolved question. With this stage of issues in cloud computing security, a decision to adopt cloud security in an organisation should be made only based on the benefits to risk ratio.The techniques of SLA coprative with cyrpotghres and trusted computing work together will find these as a good solution of security issues and will improve the security of cloud computing.

References

[1]Kaufman, L. M, "Data Security in the World of Cloud Computing." *IEEE Security and Privacy*, vol 7, no 4, pp.61-64, 2009.

[2]Kim, W. "Cloud Computing :Today and Tomorrow."*Journal of object technology*, vol 8, no 1, pp.65-72, 2009

[3]Grossman, R. "The Case for Cloud Computing." *ITPROFESSIONAL*, vol 11, no 2, pp. 23-27,2009.

[4]Mell, P. & Grance, T. "The NIST definition of cloud computing." Retrieved from http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc 2009.

[5]Leavitt, N. "Is cloud computing really ready for prime time?" *Computer*, vol *42* ,no 1, pp.15-25, 2009 Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee.org. libproxy. uoregon.edu /stamp/stamp.jsp?arnumber=04755149

[6]Erdogmus, H. (2009). "Cloud Computing: Does nirvana hide behind the nebula?" *IEEE Software*, vol *26*, no 2,pp. 4-6, 2009. Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee.org.libproxy.uoregon.edu/stamp/stamp.jsp?arnumber=04786942

[7]Leavitt, N. "Is cloud computing really ready for prime time?" *Computer* ,vol 42, no 1,pp. 15-25, 2009 Retrieved from IEEE Xplore Digital Library: http://ieeexplore.ieee.org.libproxy.uoregon.edu/stamp/stamp.jsp?arnumber=04755149

[8] Hawthorn, N. "Finding Security in the Cloud."*Computer Fraud & Security* vol 10, pp. 19-20.2009.

[9]Ryan, V. "A place in the cloud." *CFO*, vol *24*, no 8,pp. 31-35.2008

[10]Rash, W. "Is cloud computing secure? Prove it." *eWeek*, vol *26*, no 16),pp. 8-10, 2009.

[11]Hayes, B. "Cloud computing." *Communications of the ACM*, vol *51*, no.7,pp. 9-11, 2008.

[12]ISACA. (2009). "Cloud Computing: Business benefits with security, governance and assurance perspectives*".*

[13]Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., et al. (2009) " Above the Clouds: A Berkeley view of cloud computing."

[14]Gatewood, B. "Clouds on the information horizon: How to avoid the storm." *Information Management (15352897)*, vol *43*, no 4,pp. 32-36, 2009

[15]Peter Mell, Tim Grance , "Effectively and Securely Using the Cloud Computing Paradigm" *NIST, Information Technology Laboratory*, vol 10, pp. 7, 200

[16]Wyld, D. (2009). " Moving to the cloud: an introduction to cloud computing in government E-Government Series. : IBM Center for the Business of Government"

[17]Youseff, L., Butrico, M., & Da Silva, D. (2008). "Toward a unified ontology of cloud computing." *Paper presented at The Grid Computing Environments Workshop* at GCE 2008, Austin, Texas.

[18] Hand, E. "Head in the clouds." *Nature*, vol 449,pp. 963, 2007.

[19] Anderson, C. (2008). "The end of theory: The data deluge makes the scientific method obsolete." *Wired* (February 27, 2009 Retrieved June 12, 2009 from http://www.wired.com/science/discoveries/magazine/16-07/pb_theory).

[21] Beizer, D. (2009). "USA.gov will move to cloud computing" Retrieved April 15, 2009, from http://www.fcw.com/Articles/2009/02/23/USAgov-moves-to-the-cloud.aspx.

[22]Obama, B. (2009). "January 21" Retrieved May 1, 2009, fromhttp://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/.

[23]Kubicek, H. (2008). "Next generation FoI between information management and Web 2.0." Paper presented at the 2008 *International Conference on Digital Government Research*, Montreal, QC.

[24]Burroughs, J. M. "What users want: assessing government information preferences to drive information services." *Government Information Quarterly*, vol 26,pp. 203−218, 2009.

[25] Bertot, J., Jaeger, P. T., Shuler, J. A., Simmons, S. N., & Grimes, J. M. "Reconciling government documents and e-Government: Government information in policy, librarianship, and education." *Government Information Quarterly*, vol 26, pp. 433−436, 2010.

[26] Dikaiakos, M., D. Katsaros, et al. "Cloud computing: Distributed Internet Computing for IT and Scinentific Research." *IEEE Internet Computing* vol 13, no5, pp. 10-13, 2009.

[27]Weiss, A. (2007). "Computing in the Clouds." *COMPUTING* pp.16.

[28] Kaufman, L. M.."Data Security in the World of Cloud Computing." *IEEE Security and Privacy* vol 7, no 4, pp. 61-64, 2009.

[29] D. And M. Creeger. "computing 2cloud computing: An Overview."*Distributed Computing* vol 7 pp.5, 2009.

[30]William, "7 things you shoud know about the cloud computing" *EDUCAUSE*, available from:http://creativecommons.org/Licenses/by.nc.nd/3.0/ ml[accessed: 4/7/2010]

[31] X. Chu et al. Aneka: "Next-generation enterprise grid platform for e-science and e-business applications." *Proceedings of the 3rd IEEE International Conference on e-Science and Grid Computing*, 2007.

[32] J. E. Smith and R. Nair. *Virtual Machines: Versatile platforms for systems and processes*. 2005.

[33] R. Buyya and M. Murshed. "GridSim: A Toolkit for the Modeling and Simulation of Distributed Resource Management and Scheduling for Grid Computing." *Concurrency and Computation: Practice and Experience*, vol 14, pp.13-15), Wiley Press, Nov.-Dec., 2002.

[34]R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I.Brandic. "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility." *Future Generation Computer Systems*, vol 25 no 6, pp. 599-616, Elsevier Science, Amsterdam, The Netherlands, June 2009.

[35]R. Buyya1, R. Ranjan2 and R. N. Calheiros, "Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities"

[36]Cloud Security Alliance . "Security Guidance for Critical Areas of Focus in cloud computing."Retrieved Nov 25, 2009, from http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

[37]A. Sharma ,and K.Shrivastava "Privacy – Reason Enough to Reconsider a Cloud Service" 2009

[38]A Security Analysis of Cloud Computing:(http://cloudcomputing.syson.com/node/1203943

[39] Cloud Security Questions? Here are some answers (http://cloudcomputing.sys-con.com/node/1330353)

[40] Trusted Computing Group Cloud Computing and Security A Natural Match www.trustedcomputinggroup.org April 2010

[41] T.J Betcher, "Cloud Computing: Key IT related Risks and Mitigation Strategies for Consideration by IT Security Practitioners". Feb 2010

[42] Chow et al., "Cloud Computing: Outsourcing Computation without Outsourcing Control", *1stACM* Cloud Computing Security Workshop, November 2009.