International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 1, Issue 3 (july-August 2013), PP. 40-46

DATA SECURITY IN CLOUD COMPUTING AND COST ANALYSIS: REVIEW

Rajeev Kumar
Department of Computer Science & Engineering
Institute of Engineering & Technology, Alwar
Rajasthan Technical University, Kota, India

***Abstract*—This paper express the state of art in cloud computing data security. It also express the architecture development model of cloud computing with different types of layer. This paper also highlights the issues involved in data security as well as challenges which are the bottle nick of the data security. We also discussed the cost estimation in data security in consumer and provider both perspective.**

***Index Terms*— cloud computing, data security cost analysis etc.** *(key words)*

I. INTRODUCTION.

The new developments in the field of information technology offered the people enjoyment, comforts and convenience. Cloud computing is one of the latest developments in the IT industry also known as on-demand computing. It provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. It is the application provided in the form of service over the internet and system hardware in the data centers that gives these services. This technology has the capacity to admittance a common collection of resources on request. It is proving extremely striking to cash-strapped IT departments that are wanted to deliver better services under pressure. When this cloud is made available for the general customer on pay per use basis, then it is called public cloud. When customer develops their own applications and run their own internal infrastructure then is called private cloud. Integration and consolidation of public and private cloud is called hybrid cloud. But having many advantages for IT organizations cloud has some issues that must be consider during its deployment. The main concern is security privacy and trust. These issues are arises during the deployment of mostly public cloud because in public cloud infrastructure customer is not aware where the data store & how over the internet. Cloud computing" is the next natural step in the evolution of on-demand information technology services and products. Cloud Computing is a jargon term without a commonly accepted non-ambiguous scientific or technical definition. In science Cloud computing is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. The popularity of the term Cloud computing can be attributed to its use in marketing to sell hosted services in the sense of Application Service Provisioning that run Client server software on a remote location..

II. DEPLOYMENT MODELS

Cloud services can be deployed in different ways, depending on the organizational structure and the provisioning location. Four deployment models are usually distinguished, namely public, private, community and hybrid cloud service usage.

Deploying cloud computing can differ depending on requirements, and the following four deployment models have been identified, each with specific characteristics that support the needs of the services and users of the clouds in particular ways (see Figure 1).

A. Private Cloud

The cloud infrastructure has been deployed, and is maintained and operated for a specific organization. The operation may be in-house or with a third party on the premises.

B. Community Cloud

The cloud infrastructure is shared among a number of organizations with similar interests and requirements.
This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. The operation may be in-house or with a third party on the premises.

C. Public Cloud

The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.

D. Hybrid Cloud

The cloud infrastructure consists of a number of clouds of any type, but the clouds have the ability through their

interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that support the requirement to retain some data in an organization, and also the need to offer services in the cloud.

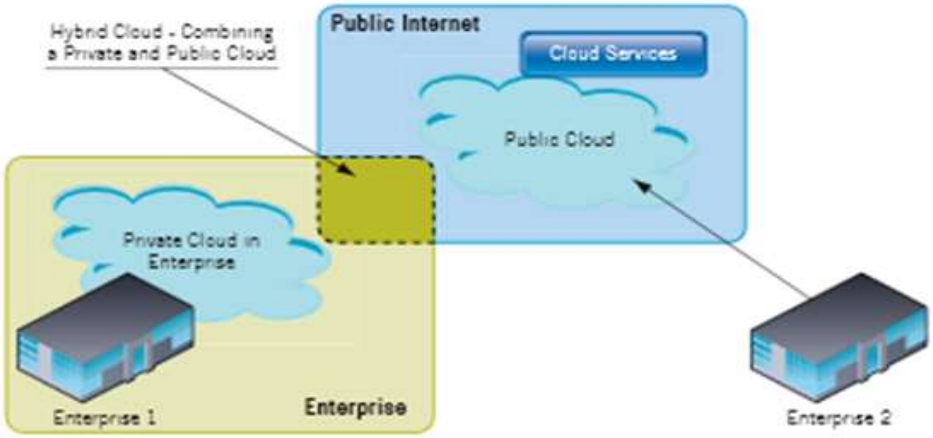

Fig.1 Public, Private, and Hybrid Cloud Deployment Example

III. ARCHITECHTURE AND DEPLOYEMENT MODEL OF CLOUD COMPUTING

Cloud computing can be classified based on the services offered and deployment models. According to the different types of services offered, cloud computing can be considered to consist of three layers.

considered to consist of three layers.

Infrastructure as a Service (IaaS) is the lowest layer that provides basic infrastructure support service.

Platform as a Service (PaaS) layer is the middle layer, which offers platform oriented services, besides providing the environment for hosting user's applications.

Software as a Service (SaaS) is the topmost layer which features a complete application offered as service on demand.

Cloud Computing distinguishes itself from other computing paradigms like grid computing, global computing, and internet computing in various aspects of on demand service provision, user centric interfaces, guaranteed QoS (Quality of Service), and autonomous system etc. A few state of the art techniques that contribute to cloud computing are:

Virtualization: It has been the underlying concept towards such a huge rise of cloud computing in the modern era. The term refers to providing an environment that is able to render all the services, supported by a hardware that can be observed on a personal computer, to the end users. The three existing forms of virtualization categorized as:

Server virtualization, Storage virtualization and Network virtualization, have inexorably led to the evolution of Cloud computing. For example, a number of underutilized physical servers may be consolidated within a smaller number of better utilized severs.

• Web Service and SOA: Web services provided services over the web using technologies like XML, Web Services Description Language (WSDL), Simple Object Access Protocol (SOAP), and Universal Description, Discovery, and Integration (UDDI). The service organisation inside a cloud is managed in the form of Service Oriented Architecture (SOA) and hence we can define SOA as something that makes use of multiple services to perform a specific task [1].

• Application Programming Interface (API): Without APIs it is hard to imagine the existence of cloud computing. The whole bunch of cloud services depend on APIs and allow deployment and configuration through them. Based on the API category used viz. control, data and application, different functions of APIs are invoked and services are rendered to the users accordingly.

• Web 2.0 /Mash-up: Web 2.0 has been defined as a technology that enables us to create web pages and allows the users to interact and collaborate as creators of user generated content in a virtual community. It enables the usage of World Wide Web technology towards a more creative and a collaborative platform [2]. Mash-up is a web application that combines data from more than one source into a single integrated storage tool.

IV. SECURITY ISSUES IN CLOUD COMPUTING:

1**. DoS attacks** comes into play when a malicious computer bombards the web server of a particular service with so many requests that the bandwidth is totally consumed with these fake requests and because of that attack the genuine user who has a

real requests is denied the possibility of getting the request completed. This is done with the help of IP spoofing and zombie computers, it works in such way that request generated by the malicious host is send to all zombie computers and which in turn send it to a particular web server hence consuming all the bandwidth since the web server will try to answer all the request and wait for the response since there is no one on the other side hence the server will wait with the open channel for the response, hence resulting in a DoS attack

Countermeasure: IP traceback and group filtering are some of the countermeasures for the DOS attack , in IP traceback , the IP of the suspected Router of client is traced back to check its origin, if not verified then the channel is blocked for it. In group filtering the packet TTL is checked along with the benchmark of the group if the TTL is more than the expected value the filtering for that IP is done.

2. **Internet connections** can be attacked in various ways. A general type of attack is called "Man-in–the-middle". The idea behind this attack is to get in between the sender and the recipient, access the traffic, modify it and forward it to the recipient. The term "Man-in-the-middle" have been used in the context of computer security since at least 1994, some different variants of this kind of attack exist, but a general definition of a man-in-the-middle attack may be described as a " Computer security breach in which a malicious user intercepts — and possibly alters — data travelling along a network. This is another issue of network security that will happen if secure socket layer (SSL) is not properly configured. For example if two parties are communicating with each other and SSL is not properly installed then all the data communication between two parties could be hack by the middle party.

Countermeasure: The proper installation of secure socket layer(SSL) is required and the secured channel should always be checked before the trusted parties are going to start the communication.

3. **Network Sniffing** Another type of attack is network sniffer, it is a more critical issue of network security in which unencrypted data are hacked through network for example an attacker can hack passwords that are not properly encrypted during communication. If the communication parties not used encryption techniques for data security then attacker can capture the data during transmission as a third party.

Countermeasure: The user should the encrypted method such as AES 128bit and triple DES to secure the data been transferred.

4. **SQL Injection Attack:** SQL injection attacks are the attacks where a hackers uses the special characters to return the data for example in SQL scripting the query end up with where clause that may be modified by adding more information in it. For example an argument value of variable y or 1==1 may cause the return of full table because 1==1is always seems to be true.

5. **Browser Security:** The next issue is Browser Security. As a client sent the request to the server by web browser the web browser have to make use of SSL to encrypt the credentials to authenticate the user.SSL support point to point communication means if there is third party, intermediary host can decrypt the data. If hacker installs sniffing packages on intermediary host, the attacker may get the credentials of the user and use in these credentials in the cloud system as a valid user.

Counter measure: countermeasure for this attack is Vendor should use WS-security concept on web browsers because WS-security works in message level that use XML encryption for continuous encryption of SOAP messages which does not have to be decrypted at mediator hosts.

6. **Cloud Malware Injection Attack**: The third issue is Cloud Malware Injection Attack, which tries to damage a spiteful service, application or virtual machine. An interloper is obligatory to generate his personal spiteful application, service or virtual machine request and put it into the cloud structure (Booth, 2004). Once the spiteful software is entered into the cloud structure, the attacker care for the spiteful software as legitimate request. If successful user ask for the spiteful service then malicious is implemented. Attacker upload virus program in to the cloud structure. Once cloud structure care for as a legitimate service the virus is implemented which spoils the cloud structure. In this case hardware damages and attacker aim is to damage the user. Once user asks for the spiteful program request the cloud throws the virus to the client over the internet. The client machine is infected by virus.

Counter measure: Counter measure for this attack is authenticity check for received messages. Store the original image file of the request by using hash function and compare it with the hash value of all upcoming service requests. In this way attacker create a legitimate hash value to deal with cloud system or to enter into the cloud system.

V. CLOUD SECURITY ISSUES AND CHALLENGES

Cloud computing is a emerging technology with shared resources, lower cost and rely on pay per use according to the user demand. Due to many characteristics it has effect on IT budget and also impact on security, privacy and security issues .In this section all these issues are discussed. All those CSPs who wish to enjoy this new trend should take care of these problems. As Pakistan is developing country with no any proper IT strategy, a CSP should give their full attention to security aspect of cloud because it is a shared pool of resources. Customer not know where the data are stored, who manage data and other vulnerabilities that can occur. Following are some issues that can be faced by CSP while implementing cloud services.

A. Privacy Issue

It is the human right to secure his private and sensitive information. In cloud context privacy occur according to the cloud deployment model [3]. In Public cloud (accessed through the Internet and shared amongst different consumers) is one of the dominant architecture when cost reduction is concerned,

but relying on a CSP to manage and hold customer information raises many privacy concerns and are discussed under:

B. Lack of user control

In SAAS environment service provider is responsible to control data. Now how customer can retain its control on data when information is processed or stored. It is legal requirement of him and also to make trust between customer and vendor [4] . In this new paradigm user sensitive information and data is processed in 'the cloud' on systems having no any, therefore they have danger of misuse, theft or illegal resale. Adding more, this is not patent that it will be possible for a CSP to guarantee that a data subject can get access to all his/her PII, or to comply with a request for deletion of all his/her data. This can be difficult to get data back from the cloud, and avoid vendor lock-in [5].

C. Unauthorized Secondary Usage

One of the threats can occur if information is placed for illegal uses. Cloud computing standard business model tells that the service provider can achieve profits from authorized secondary uses of users' data, mostly the targeting of commercials [6]. Now days there are no technological barriers for secondary uses. In addition, it has the connected issue of financial flexibility of the CSPs: for example, possibility of vendor termination, and if cloud computing provider is bankrupted or another company get data then what would happen [7]

D. Transborder Data Flow and Data Proliferation

One of the attribute of cloud is Data proliferation and which involves several companies and is not controlled and managed by the data owners. Vendor guarantee to the ease of use by copy data in several datacentres. This is very difficult to ensure that duplicate of the data or its backups are not stored or processed in a certain authority, all these copies of data are deleted if such a request is made. Due to movement of data, CP exacerbate the trans-border data flow matter because it can be tremendously difficult to ascertain which specific server or storage device will be used, as the dynamic nature of this technology [8].

E. Dynamic provision

Cloud has vibrant nature so there is no clear aspect that which one is legally responsible to ensure privacy of sensitive data put by customer on cloud [9].

F. Security

Public cloud not only increases the privacy issue but also security concern. Some security concerns are described below:

G. Access

It has the threat of access sensitive information. The risk of data theft from machine has more chances in cloud environment data stored in cloud a long time duration any hacker can access this data [10].

H. Control over data lifecycle

To ensure the customer that it has control over data, if it remove or delete data vendor cannot regain this data. In cloud IAAS and PAAS models virtual machine are used that process and then media wiped but still there is no surety that next user cannot get that data [11].

I. Availability and backup

There is no any surety of availability and back up of data in this environment. In business backup is one of the important consideration [10].

J. Multi-tenancy

It is feature of SAAS that one program can run to multiple machines. CSP use multi-tenant application of cloud to reduce cost by using virtual machine but it increase more vulnerability [10].

K. Audit

To implement internal monitoring control CSP need external audit mechanism .But still cloud fails to provide auditing of the transaction without effecting integrity [12].

L. Trust

Trust is very necessary aspect in business. Still cloud is failed to make trust between customer and provider. So the vendor uses this marvellous application should make trust. Weak trust relationship and lack of customer trust cause many problems during deployment of cloud services [13]

M. Mitigation Steps

This section includes mitigation steps and some solution to overcome the issues discussed in previous section. It provides guidelines to the companies that offer cloud services .It will helpful to them to make proper strategy before implementing cloud services. There are some alleviations to reduce the effect of security, trust and privacy issue in cloud environment. There are many adoption issues like user get privilege to control data cause low transaction performance, companies are worried from cybercrimes and as Pakistan is now going to developed so the Internet speed also effect the performance, virtual machines are taking milliseconds to encrypt data which is not sufficient and to avoid risk there is contract between parties to access data [14]. So mitigate such type of problems some action should take place. Some steps are listed below:

Build up an iterative policy for relocation from traditional environment to Cloud environment. Vendors in Pakistan should follow proper strategy moving from their existing system to this new evolution.

As this upcoming trend reduce cost but be careful to select possible solutions to avoid problems in this computing and calculate the effect on the system just not consider the outlay.

Providers should be aware regarding new changes and assure that customers access privileges are limited.

Cloud is a shared pool of resource. Discover the linked service providers that wants to connected to particular Cloud service provider to query, which provider has right to use facts and data .System for monitoring should be request for exclusion.Service provider should tell customer for managing polices for security beside provider's owned policies, with in the duration of services.

Make it sure, that the data being transferred is protected and secured by standard security techniques and managed by appropriate professionals .

N. Proposed Solutions

The Table 1 shown below gives a look on the solutions that are helpful to the cloud customer and companies offer services in Pakistan with secure and trusty environment.

Solution	Description
Data Handling Mechanism	• Classify the confidential Data. • Define the geographical region of data. • Define policies for data destruction.
Data Security Mitigation	• Encrypting personal data. • Avoid putting sensitive data in cloud.
Design for Policy	• Fair information principles are applicable.
Standardization	• CSP should follow standardization in data tracking and handling.
Accountability	• For businesses having data lost, leakage or privacy violation is catastrophic. • Accountability needs in legal and technical. • Audit is need in every step to increase trust. • All CSP make contractual agreements.
Mechanism for rising trust	• Social and technological method to raise trust. • Joining individual personal rights, preferences and conditions straightforwardly to uniqueness of data. • Devices connected should be under control by CSP. • Use intelligent software.

Table No. 1 Proposed Solutions

VI. TOP THREATS TO CLOUD COMPUTING

1: Account or Service & Hijacking
2: Insecure Interfaces and APIS
3: Malicious Insiders
4: Shared Technology Issues
5: Data Loss or Leakage

A. WHAT IS ACTUALLY HAPPENING?

When a user opens his cloud platform and creates a file in that, which may contain some essential data. When the user logs off his cloud platform the data that is created by the user will be stored in the cloud provider's server in an encrypted form. When the user re login into his cloud platform the data will be decrypted from the server and given to the server.

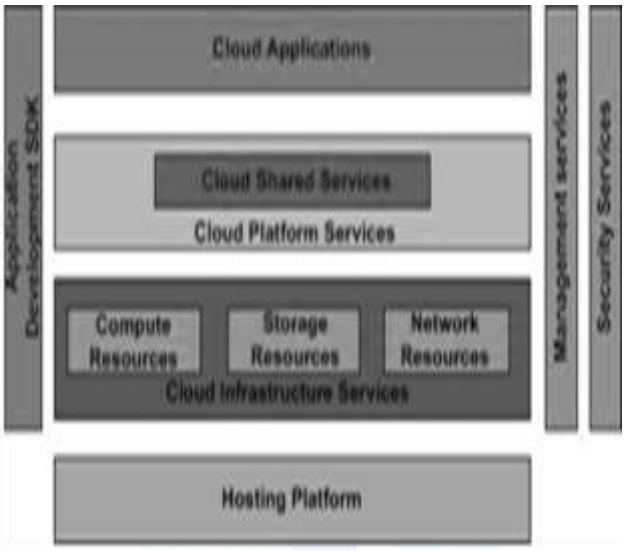

Fig.2 Cloud Architecture

B. ISSUES

1) The biggest issue now is the server can be hacked by the hackers and the data can be decrypted. Hence, user data is lost.

2) From the above figure, it is clear that in the cloud computing each and every component such as software, data storage is provided as a service.

3) From the above figure, it is clear that in the cloud computing each and every component such as software, data storage is provided as a service.

4) Although it reduces the cost of hardware it is not much reliable because of the data that is being directly stored in provider server.

VII. CLOUD COMPUTING AND COST

The economic appeal of Cloud Computing is often mentioned as "converting capital expenses to operating expenses" 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. There are different cost models available in the market for Cloud Computing. However, the most used model is discussed by Armbrust,[13] which is a short term billing model. 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.

VIII. 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) [13] 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 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 overweighed 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). Perunit pricing is mostly used with data transfer and memory usage (Youseff et al., 2008). 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).

IX. 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).

X. CLOUD COMPUTING'S COST EFFECT

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

XI. CONCLUSION AND DISCUSSION

Many publications have dealt with various types of security requirements in cloud computing but not all types have been explored in sufficient depth. It is also hard to understand which types of requirements have been under-researched and which are most investigated. So with the help of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating. This paper's goal is to provide a comprehensive and structured overview of cloud computing security requirements and solutions.

The main motivation for this is largely due to fear of encryption services getting outlawed, and copyright owners who want to track confidential and intellectual property copyright against unauthorized access and use in digital materials. We carried out a systematic review and identified security requirements from previous publications that we classified in nine sub-areas: Access Control, Attack/Harm Detection, Non-repudiation, Integrity, Security Auditing, Physical Protection, Privacy, Recovery, and Prosecution. We found that (i) the least researched sub-areas are non-repudiation, physical protection, recovery and prosecution, and that (ii) access control, integrity and auditability are the most researched sub-areas.

REFERENCES

[1] K. Popovic, Z. Hocenski, ‖ Cloud Computing security issues and challenges ‖ , MIPRO, Proceedings of the 33rd International Convention, 2010.

[2] Z. Shen, L. Li, F. Yab, X. Wu, —Cloud Computing system asked on Trusted computing platform ‖ , International Conference on Intelligent Computation technology and Automation, 2010.

[3] Andreas Tolk. 2006. What Comes After the Semantic Web - PADS Implications for the Dynamic Web. 20th Workshop on Principles of Advanced and Distributed Simulation (PADS '06). IEEE Computer Society, Washington, DC, USA

[4] "Cloud Computing: Clash of the clouds". The Economist. 2009-10-15. Retrieved 2009-11-03."Gartner Says Cloud Computing Will Be As Influential As E-business". Gartner. Retrieved 2010-08-22.

[5] Gruman, Galen (2008-04-07). "What cloud computing really means". InfoWorld. Retrieved 2009-06-02.

[6] Jeff Bezos' Risky Bet". Business Week

[7] Keep an eye on cloud computing, Amy Schurr, Network World, 2008-07-08, citing the Gartner report, "Cloud Computing Confusion Leads to Opportunity". Retrieved 2009-09-11.

[8] 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.

[9] 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).

[10] B Rochwerger, J Caceres, RS Montero, D Breitgand, E Elmroth, A Galis, E Levy, IM Llorente, K Nagin, Y Wolfsthal, E Elmroth, J Caceres, M Ben-Yehuda, W Emmerich, F Galan. "The RESERVOIR Model and Architecture for Open Federated Cloud Computing", IBM Journal of Research and Development, Vol. 53, No. 4. (2009)

[11] D Kyriazis, A Menychtas, G Kousiouris, K Oberle, T Voith, M Boniface, E Oliveros, T Cucinotta, S Berger, "A Real-time Service Oriented Infrastructure", International Conference on Real-Time and Embedded Systems (RTES 2010), Singapore, November 2010

[12] Keep an eye on cloud computing, Amy Schurr, Network World, 2008-07-08, citing the Gartner report, "Cloud Computing Confusion Leads to Opportunity". Retrieved 2009-09-11.

[13] 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.

[14] S. Nivetha, —Assessing the Risks and Opportunities of Cloud Computing – Defining Identity Management Systems and Maturity Models ‖ , International Conference on Computing and Control Engineering, 2012.