ISSN:0975-9646

A Study of the Issues and Security of Cloud Computing

Shaurya Gupta, Piyush Gupta

Department of Computer Science and Engineering
Jagannath University, Jaipur

***Abstract*--The paper identifies the issues and the solution to overcome these problems. Cloud computing is a subscription based service where we can obtain networked storage space and computer resources. This technology has the capacity to admittance a common collection of resources on request. It is the application provided in the form of service over the internet and system hardware in the data centers that gives these services. 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. There are various issues that need to be dealt with respect to security and privacy in a cloud computing scenario [4].**

***Keywords*--Cloud, Issues, Security, Privacy, Resources, Technology**.

I. INTRODUCTION

Cloud computing is latest trend in IT world. It is Internet-based computing, whereby shared resources, software and information, are provided to computers and other devices on-demand, like the electric grid. 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. It has many open issues some are technical that includes scalability, elasticity ,data handling mechanism, reliability, license software, ownership, performance, system development and management and non-technical issues like legalistic and economic aspect. The new concept of Cloud Computing offers dynamically scalable resources provisioned as a service over the Internet and therefore promises a lot of economic benefits to be distributed among its adopters [2,5]. Depending on the type of resources provided by the Cloud, distinct layers can be define According to the different types of services offered, cloud computing can be considered to consist of three layers .

Software as a Service (SaaS) is the topmost layer which features a complete application offered as service on demand SaaS ensures that the complete applications are hosted on the internet and users use them. The payment is being made on a pay-per-use model. It eliminates the need to install and run the application on the customer's local computer, thus alleviating the customer's burden for software maintenance.

In SaaS, there is the Divided Cloud and Convergence coherence mechanism whereby every data item has either the "Read Lock" or "Write Lock". Two types of servers are used by SaaS: the Main Consistence Server (MCS) and Domain Consistence Server (DCS). Cache coherence is achieved by the cooperation between MCS and DCS. In SaaS, if the MCS is damaged, or compromised, the control over the cloud environment is lost [3]. Hence securing the MCS is of great importance.

Platform as a service (PaaS) approach offering also includes a software execution environment. As for example, there could be a PaaS application server that enables the lone developers to deploy web-based applications without buying actual servers and setting them up. PaaS model aims to protect data, which is especially important in case of storage as a service. In case of congestion, there is the problem of outage from a cloud environment. Thus the need for security against outage is important to ensure load balanced service. The data needs to be encrypted when hosted on a platform for security reasons [4].

Infrastructure as a service (IaaS) refers to the sharing of hardware resources for executing services, typically using Virtualization technology. With IaaS approach, potentially multiple users use available resources. The resources can easily be scaled up depending on the demand from user and they are typically charged for on a pay-per-use basis. The resources are all virtual machines, which has to be managed. Thus a governance framework is required to control the creation and usage of virtual machines. This also helps to avoid uncontrolled access to user's sensitive information [4].

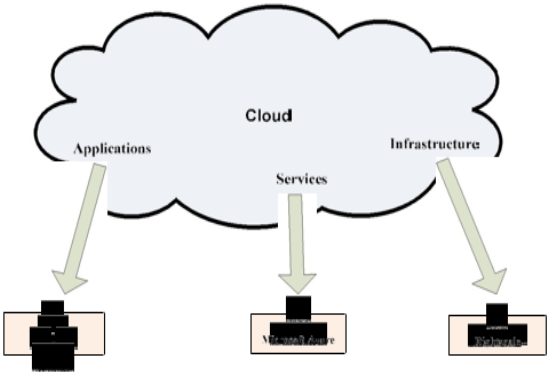

Figure1:- A simple cloud computing model with the three basic cloud services involved.

Fig.1 shows the basic cloud architecture depicting the various service providers associated with different elements of cloud. Irrespective of the above mentioned service models, cloud services can be deployed in four ways depending upon the customers' requirements:

A. Public Cloud: A cloud infrastructure is provided to many customers and is managed by a third party. Multiple enterprises can work on the infrastructure provided, at the same time. Users can dynamically provision resources

through the internet from an off-site service provider. Wastage of resources is checked as the user pays for whatever they use.

B. Private Cloud: Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider. This uses the concept of virtualization of machines, and is a proprietary network

C. Community cloud: Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider.

D. Hybrid Cloud: A composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other[1,3,4].

Service based Cloud Computing:-

Cloud Computing distinguishes itself from other computing paradigms like grid computing, global computing, internet computing in the various aspects of On Demand Service Provision, User Centric Interfaces, guaranteed QoS, Autonomous system , etc. [3]. A few state of the art techniques that contribute to the cloud computing are:

A. 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 able to render all the services, being 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 lead to the evolution of Cloud computing. As for example, a number of underutilized physical servers may be consolidated within a smaller number of better utilized servers.

B. 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 organization 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.

C. Application Programming Interface (API): Without API's it's hard to believe the existence of cloud computing. The whole bunches of cloud services depend on API's and allow deployment and configuration through them. Based on the API category used viz. Control, Data and Application API's different functions are being c ontrolled and services rendered to the users.

D. Web 2.0 and mash-up: Web 2.0 has been defined as a technology, enabling us to create web pages that don't limit a user to viewing only; in fact it allows the users to make dynamic updates as well. It enables the usage of World Wide Web technology towards a more creative and a collaborative platform. Mash-up is a web application that combines data from more than one source into a single integrated storage tool [4,5].

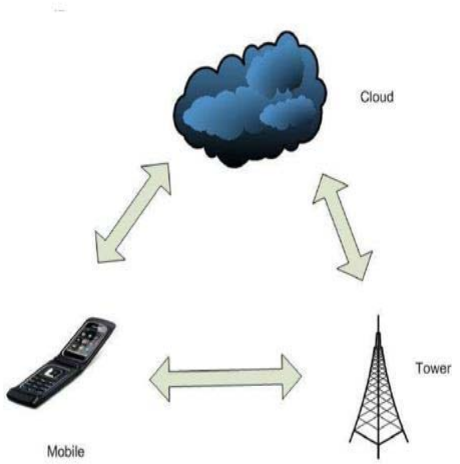

Figure 2:- A Mobile Cloud Computing Scenario

II. BARRIERS TO CLOUD COMPUTING.

In spite of being a hot topic, there are certain aspects behind the fact that many organizations are yet not confident of moving into the cloud. Certain loopholes in its architecture have made cloud computing vulnerable to various security and privacy threats. A few issues limiting the boundaries of this transformational concept are:

A. Privacy and Security

The fundamental factor defining the success of any new computing technology resides on the term how much secure it is. Whether the data residing in the cloud is secure to a level so as to avoid any sort of security breach or it is more secure to store the data away from cloud in our own personal computers or hard drives? At-least we can access our hard drives and systems whenever we wish to, but cloud servers could potentially reside anywhere in the world and any sort of internet breakdown can deny us access to the data lying in the cloud. Such companies argue that the data on their servers is inherently more secure than data residing on a myriad of personal computers and laptops. However, it is also a part of cloud architecture, that the client data will be distributed over these individual computers regardless of where the base repository of data is ultimately stored. There have been instances when their security has been invaded and the whole system had been down for hours.

In case of a public-cloud computing scenario, we have multiple security issues that need to be addressed in comparison to a private cloud computing scenario [1]. A public cloud acts as a host of a number of virtual machines, virtual machine monitors, supporting middleware etc. Besides, privacy needs to be maintained as there are high chances of an eavesdropper to be able to sneak in.

B. Performance, Latency and Reliability

Latency has always been an issue in cloud computing with data expected to flow around different clouds. The other factors that add to the latency are encryption and decryption of the data when it moves around unreliable and public networks, congestion, packet loss and windowing. Congestion adds to the latency when the traffic flow through the network is high and there are

many requests (may be of same priority) that need to be executed at the same time.

C. Portability and Interoperability

Organizations may need to change the cloud providers and there have been cases when companies can't move their data and applications if they find another cloud platform they like better than the one they are using. In some cases, different cloud platforms are used for a particular application or different cloud platforms have to interact with each other for completing a particular task. The internal infrastructure of the organization is needed to maintain a balance to handle the interoperability between different cloud platforms[1, 2]. The risk of outsourced services going out of control is too much in a hybrid public and private cloud environment. All data has to be encrypted for proper security, and key management becomes a difficult task in such situations. A cloud security management model is discussed in this paper to serve as a standard for designing cloud security management tools. The model uses four interoperating layers for managing the cloud security. Thus we see that although the buzz of cloud computing prevails everywhere because of the multi-fold features and facilities provided by it, still there are issues that are needed to be solved in order to reach the landmarks set by it as to gain access to the hardware and application resources for a better functioning IT world.

D. Data-Breach through Fiber Optic Networks

It has been noticed that the security risks for the data in transit has increased over the last few years. Data transitioning is quite normal now-a-days and it may include multiple data-centers and other cloud deployment models such as public or private cloud. Security of the data leaving a data-center to another data-center is a major concern as it has been breached quite a number of times in the recent times.

This data transfer is done over a network of fiber-optic cables which were considered to be a safe mode of data-transfer, until recently an illegal fiber eavesdropping device in Telco Verizon's optical network placed at a mutual fund company was discovered by US Security forces. There are devices that can tap the data flow without even disturbing it and accessing fiber, through which data is being transferred. They generally are laid underground and hence it should not be a tough job accessing these fiber-optic cables. And hence it becomes quite important a factor to ensure data security over the transitioning networks.

E. Data Storage over IP Networks

Online data storage is becoming quite popular now-a-days and it has been observed that majority of enterprise storage will be networked in the coming years, as it allows enterprises to maintain huge chunks of data without setting up the required architecture. Although there are many advantages of having online data storage, there are security threats that could cause data leakage or data unavailability at crucial hour. Such issues are observed more frequently in the case of dynamic data that keeps flowing within the cloud in comparison to static data. Depending upon the various levels of operations and storage provided, these networked devices are categorized into SAN (Storage area network) and NAS (network- attached storage) and since these storage networks reside on various servers [4, 5], there are multiple threats or risks attached to them. The three threat zones that may affect and cause the vulnerability of a storage network have been discussed in this paper, besides these, from them a mobile cloud computing scenario, we may see that unlike cloud computing there are several additional challenges that need to be addressed to enable MCC reach its maximum potential:

1)Network accessibility: Internet has been the major factor towards the cloud computing evolution and without having the network access it won't be possible to access the internet and hence the inability to access the mobile cloud limiting the available applications that can be used.

2)Data Latency: Data transfer in a wireless network is not as continuous and consistent as it is in case of a dedicated wired LAN. And this inconsistency is largely responsible for longer time intervals for data transfer at times. Also, the distance from the source adds up to the longer time intervals observed in case of data transfer and other network related activities because of an increase in the number of intermediate network components.

3)Dynamic Network monitoring and Scalability: Applications running on mobiles in a mobile cloud computing platform should be intelligent enough to adapt to the varying network capacities and also they should be accessible through different platforms without having suffered any loss in the data. Sometimes, a user while working on a smart phone may need to move on to a feature phone and when (s)he accesses the application which (s)he was working on through her/his smart phone, (s)he should not face any data loss.

***4)Confidentiality of mobile cloud-based data sharing*:** The confidential data on mobile phones using cloud-based mobile device support might become public due to a hacked cloud provider. The root-level access to cloud services and information can be easily accessed from a stolen mobile device. If the stolen device belongs to a system administrator, they may even provide direct and automated access to highly confidential information[2, 5].

III. THREATS TO SECURITY IN CLOUD COMPUTING

The chief concern in cloud environments is to provide security around multi-tenancy and isolation, giving customers more comfort besides "trust us" idea of clouds. There has been survey works reported that classifies security threats in cloud based on the nature of the service delivery models of a cloud computing system. However, security requires a holistic approach. Service delivery model is one of many aspects that need to be considered for a comprehensive survey on cloud security. Security at different levels such as Network level, Host level and Application level is necessary to keep the cloud up and running continuously. In accordance with these different Levels, various types of security breaches may occur.

A. Basic Security

Web 2.0, a key technology towards enabling the use of Software as a Service (SaaS) relieves the users from tasks

like maintenance and installation of software. It has been used widely all around. As the user community using Web 2.0 is increasing by leaps and bounds, the security has become more important than ever for such environment.

1) *SQL injection attacks*:-

SQL injection attacks, are the one in which a malicious code is inserted into a standard SQL code and thus the attackers gain unauthorized access to a database and become able to access sensitive information. Sometimes the hacker's input data is misunderstood by the web-site as the user data and allows it to be accessed by the SQL server and this lets the attacker to have know-how of the functioning of the website and make changes into that. Various techniques like: avoiding the usage of dynamically generated SQL in the code, using filtering techniques to sanitize the user input etc to check the SQL injection attacks.

2) *Cross Site Scripting (XSS) attacks*

Cross Site Scripting (XSS) attacks, which inject malicious scripts into Web contents have become quite popular since the inception of Web 2.0. Based on the type of services provided, a website can be classified as static or dynamic. Static websites don't suffer from the security threats which the dynamic websites do because of their dynamism in providing multi-fold services to the users.

B. Network Level Security

Networks are classified into many types like: shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. To ensure network security following points such as: confidentiality and integrity in the network, proper access control and maintaining security against the external third party threats should be considered while providing network level security.

1) Sniffer attacks

These types of attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network [4].

2) Issue of reused IP addresses

Each node of a network is provided an IP address and hence an IP address is basically a finite quantity. A large number of cases related to re-used IP-address issue have been observed lately. When a particular user moves out of a network then the IP-address associated with him (earlier) is assigned to a new user. This sometimes risks the security of the new user as there is a certain time lag between the change of an IP address in DNS and the clearing of that address in DNS caches [1].

3) BGP prefix hijacking

Prefix hijacking is a type of network attack in which a wrong announcement related to the IP addresses associated with an Autonomous system (AS) is made and hence malicious parties get access to the untraceable IP addresses. These ASs communicate using the Border Gateway Protocol (BGP) model. Sometimes, due to some error, a faulty AS may broadcast wrongly about the IPs associated with it. In such case, the actual traffic gets routed to some IP other than the intended one. Hence, data is leaked or reaches to some other destination that it actually should not. An autonomous security system for autonomous systems has been explained in.

C. Application Level Security

Application level security refers to the usage of software and hardware resources to provide security to applications such that the attackers are not able to get control over these applications and make desirable changes to their format. Now a days, attacks are launched, being disguised as a trusted user and the system considering them as a trusted user, allow full access to the attacking party and gets victimized. The reason behind this is that the outdated network level security policies allow only the authorized users to access the specific IP address. With the technological advancement, these security policies have become obsolete as there have been instances when the system's security has been breached, having accessed the system in the disguise of a trusted user. With the recent technological advancements, it's quite possible to imitate a trusted user and corrupt entire data without even being noticed. Hence, it is necessary to install higher level of security checks to minimize these risks.

1) Security concerns with the hypervisor

Cloud Computing rests mainly on the concept of virtualization. In a virtualized world, hypervisor is defined as a controller popularly known as virtual machine manager (VMM) that allows multiple operating systems to be run on a system at a time, providing the resources to each operating system such that they do not interfere with each. As the number of operating systems running on a hardware unit increase, the security issues concerned with those that of new operating systems also need to be considered. Because multiple operating systems would be running on a single hardware platform, it is not possible to keep track of all and hence maintaining all the operating systems secure is difficult. It may happen that a guest system tries to run a malicious code on the host system and bring the system down or take full control of the system and block access to other guest OS. It cannot be denied that there are risks associated with sharing the same physical infrastructure between a set of multiple users, even one being malicious can cause threats to the others using the same infrastructure, and hence security with respect to hypervisor is of great concern as all the guest systems are controlled by it

2) Denial of service attacks and distributed denial of service attacks

A DoS attack is an attempt to make the services assigned to the authorized users unable to be used by them. In such an attack, the server providing the service is flooded by a large number of requests and hence the service becomes unavailable to the authorized user.

DDoS may be called an advanced version of DOS in terms of denying the important services running on a server by

flooding the destination sever with an umpteen number of packets such that the target server is not able to handle it [1]. In DDoS the attack is relayed from different dynamic networks which have already been compromised unlike DOS. The attackers have the power to control the flow of information by allowing some information available at certain times. Thus the amount and type of information available for public usage is clearly under the control of the attacker.

3) Backdoor and debug options

A common habit of the developers is to enable the debug option while publishing a web-site. This enables them to make developmental changes in the code and get them implemented in the web-site. Since these debug options facilitate back-end entry to the developers, and sometimes these debug options are left enabled unnoticed, this may provide an easy entry to a hacker into the web-site and let him make changes at the web-site level [2].

IV. DATA STORAGE AND SECURITY.

Many cloud service providers provide storage as a form of service. They take the data from the users and store them on large datacenter, hence providing users a means of storage. Although these cloud service providers say that the data stored in the cloud is utmost safe but there have been cases when the data stored in these clouds have been modified or lost may be due to some security breach or some human error [2,4].

Various cloud service providers adopt different technologies to safeguard the data stored in their cloud. But the question is: Whether the data stored in these clouds is secure enough against any sort of security breach? The virtualized nature of cloud storage makes the traditional mechanisms unsuitable for handling the security issues. These service providers use different encryption techniques like public key encryption and private key encryption to secure the data resting in the cloud.

A similar technique providing data storage security, utilizing the homo-morphed token with distributed verification of erasure-coded data has been discussed in. Trust based methods are useful in establishing relationships in a distributed environment. A domain based trust-model has been proposed to handle security and interoperability in cross clouds. Every domain has a special agent for trust management. It proposes different trust mechanisms for users and service providers.

Another major issue that is mostly neglected is of Data-Reminisce. It refers to the data left out in case of data transfer or data removal. It causes minimal security threats in private cloud computing offerings, however severe security issues may emerge out in case of public cloud offerings as a result of data-reminisce [1].

Various cases of cloud security breach came into light in the last few months. Cloud based email marketing services company, Epsilon suffered the data breach, due to which a large section of its customers including JP Morgan Chase, Citibank, Barclays Bank, hotel chains such as Marriott and Hilton, and big retailers such as Best Buy and Walgreens were affected heavily and huge chunk of customer data was exposed to the hackers which includes customer email ids and bank account details.

Another similar incident happened with Amazon causing the disruption of its EC2 service. The damage caused had proved to be quite costly for both the users and the system administrators. Popular sites like: Quora, Four-Square and Reedit were the main sufferers. The above mentioned events depict the vulnerability of the cloud services.

Another important aspect is that the known and popular domains have been used to launch malicious software or hack into the companies' secured database. A similar issue happened with Amazon's S3 platform and the hackers were able to launch corrupted codes using a trusted domain and hence the question that arises now is who to be provided the "trusted" tag. It proved that Amazon is prone to side-channel attacks, and a malicious virtual machine, occupying the same server as the target, can easily gain access to confidential data. The question is: whether any such security policy should be in place for these trusted users as well?

An incident relating to the data loss occurred last year with the online storage service provider "Media max" also known as "The Linkup" when due to system administration error, active customer data was deleted, leading to the data loss. SLA's with the Cloud Service providers should contain all the points that may cause data loss either due to some human or system generated error. Hence, it must be ensured that redundant copies of the user data should be stored in order to handle any sort of adverse situation leading to data loss.

Virtualization in general increases the security of a cloud environment. With virtualization, a single machine can be divided into many virtual machines, thus providing better data isolation and safety against denial of service attacks. The VMs provide a security test-bed for execution of untested code from un-trusted users. A hierarchical reputation system has been proposed in the paper for managing trust in a cloud environment.

V. CLOUD SECURITY ISSUES AND CHALLENGES.

Cloud computing is an 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 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 [2].

Privacy Issue:-

It is the human right to secure his private and sensitive information. 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 [2,5]:

A. Lack of user control. In SAAS environment service

provider is responsible to control data. It is legal requirement to make trust between customer and vendor. 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 Personnel information, 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 [2, 4].

B. 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 .Now a 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 [3, 5].

Security:-

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

A. 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.

B. 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.

C. 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 [4, 5].

D. Multi-tenancy

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

VI. PROPOSED SOLUTIONS.

Table: Proposed Solutions

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.

VII. CONCLUSION.

Cloud computing is latest development that provides easy access to high performance computing resources and storage infrastructure through web services. Cloud computing delivers the potential for efficiency, cost savings and improved performance to governments, organizations, private and individual users. It also offers a unique opportunity to developing countries to get closer to developed countries. Developing countries like Pakistan can take the benefits of cloud computing by implementing it in its e-government projects. The paper addresses the issues that can arise during the deployment of cloud services. After identify these problems some steps are explained to mitigate these challenges and solutions to solve the problems.

REFERENCES

[1] Meiko Jenson and luigi lo lacono "On Technical Security Issue in Cloud Computing" ,2009 IEEE International conference on cloud computing.

[2] Cong wang and wenjing lou "Privacy Preserving public auditing for data storage security in cloud computing ",Technical program at IEEE INFOCOM 2010.

[3] Ramgovind s and Smith E "The Management of security in colud computing" .

[4] Cloud Computing: A Practical Approach Anthony T. Velte Toby J. Velte, Robert Elsenpeter, McGraw- Hill Publication, ISBN: 978-0-07-162695-8

[5] Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online, by Michial miller, Que Publishing, ISBN-13: 978-0-7897-3803-5