International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 5– No.7,May 2013 – www.ijais.org

Security Threats with Associated Mitigation Techniques in Cloud Computing

Mohsin Nazir
Department of Information Technology
Central University of Kashmir, India

Mirza Shuja Rashid
Department of Computer Sciences
NIELIT, Srinagar (J&K), India

ABSTRACT
Cloud Computing emerges as one of the hottest topic in the field of information technology. Nowadays not just large organizations, but even small and medium size businesses are looking forward to adopt an economical computing resource for their business application, i.e. by introducing a new concept of cloud computing in their environment. Basically it's a new concept of providing virtualized resources to the consumers. Cloud Computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually Cloud Computing services are delivered by a third party provider who owns the infrastructure.Consumers can request a cloud for services, applications, solutions and can store large amount of data from different location. Cloud Computing holds the potential to eliminate the requirements for setting up of high-cost computing infrastructure for IT-based solutions and services that theindustry uses. It promises to provide a flexible IT architecture; accessible through internet from lightweight portable devices.This would allow multi-fold increase in the capacity and capabilities of the existing and new software. This new economic model for computing has found fertile ground and is attracting massive global investment. Many industries, such as banking, healthcare and education are moving towards the cloud due to the efficiency of services provided by the pay-per-use pattern based on the resources such as processing power used, transactions carried out, bandwidth consumed, data transferred, or storage space occupied etc. Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security in Cloud Computing is an importantand critical aspect, and has numerous issues and problem related to it. Cloud service provider and the cloudservice consumer should make sure that the cloud is safe enough from all the external threats so that thecustomer does not face any problem such as loss of data or data theft. There is also a possibility where amalicious user can penetrate the cloud by impersonating a legitimate user, thus infecting the entire cloud andaffects many customers who are sharing the infected cloud. This research paper outlines what cloud computing is, the various cloud models and the parameters that affect thesecurity of the cloud. This extensive research also aims to elaborate the possible security attacks and the security issues that arise in a cloud computing frame work. It focuses on technical security issues arising from the usage of cloud services and also provides an overview of key security issues related to cloud computing with the view of a secure cloud architecture environment.

Keywords
Cloud Computing, Software as a Service (SaaS), Platform as a Service PaaS), Infrastructure as a Service (IaaS), Mobile Cloud Computing (MCC), Security issues, Denial of Service (DoS), Distributed Denial of Service (DDoS), Secure Cloud Architecture.

1. INTRODUCTION
Cloud computing is a very broad term used for the recent development of internet-based computing. According to U.S National Institute of Standards and Technology (NIST), *"Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage devices and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* [41]. In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet [22].In such an environment users need not own the infrastructure for various computing services. In fact, they can be accessed from any computer in any part of the world. This integrates features supporting high scalability and multi-tenancy, offering enhanced flexibility in comparison to the earlier existing computing methodologies. It can deploy, allocate or reallocate resources dynamically with an ability to continuously monitor their performance [41]. Main goal of the Cloud Computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels [16, 27].

Even though there are numerous variations on the definition of Cloud Computing, some basic principles characterize this emerging computing paradigm. Cloud Computing provides technological capabilities—generally maintained off premises— that are delivered on demand as a service via the Internet. Given that a third party owns and manages public cloud services, consumers of these services do not possess resources in the cloud model but pay for them on a per-use basis. Thus virtualization of the resources is the key concept [55]. In the real scenario, they are renting the physical infrastructure, platforms and applications within a shared architecture. Cloud offerings can vary from virtual infrastructure, computing platforms, centralized data centres to end-user Web-Services and Web applications to enormous other focused computing services [37].

Many companies developing and offering Cloud Computing products and services but have not properly considered the implications of processing, storing and accessing data in a shared and virtualized environment. In fact, many developers of cloud-based applications struggle to include security. In other cases, developers simply cannot provide real security with currently affordable technological capabilities [41]. There are three important things to be mentioned about cloud security. Firstly, cloud security is almost exactly like internal security. The security tools that are used now-a-days to protect the internal network cloud, also used to protect data in the cloud. Secondly, for remaining financially competitive, some of these security technologies should be moved to the

cloud. Thirdly, if a quality cloud service provider is selected, the security in the cloud will be as good as or better than the current security in most cases. This paper discusses the security threats present in the cloud, and their countermeasures and also proposes a secure architecture for the cloud implementation.

2. OVERVIEW OF CLOUD COMPUTING

Cloud Computing is a general term for anything that involves delivering hosted services over the Internet [38]. After studying 20 definitions Vaquero et al., (2009) come up with a minimum definition containing essential characteristics *"Clouds are a large pool of easily and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically re-configured 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 service-level agreements"*. Instead of a static system architecture, Cloud Computing supports the ability to dynamically scale up and quickly scale down, offering cloud consumers high reliability, quick response times, and the flexibility to handle traffic fluctuations and demand [34, 37]. Cloud Computing also supports multi tenancy, providing systems configured in such a way that they can be pooled to be shared by many organizations or individuals [15, 37]. Virtualization technology allows cloud vendors to convert one server into many virtual machines, thereby eliminating client-server computing with single-purpose systems [26]. This maximizes hardware capacity and allows customers to leverage economies of scale [34]. Resources on the cloud can be used by the client and deployed by the vendor such as Amazon, Google, IBM, Salesforce, Zoho, Rackspace, Microsoft etc.

Benefits of Cloud computing are enormous. The most important one is that the customers don't need to buy the resource from a third party vendor, instead they can use the resource and pay for it as a service thus helping the customer to save time and money [37]. Cloud Computing may also be applied to solve problems in many domains of Information Technology like GIS (Geographical Information Systems), Scientific Research [13], e-GovernanceSystems [29], Decision Support Systems [62], ERP [26], Web Application Development [33], Mobile Technology [53] etc.

2.1 DEPLOYMENT MODELS

A deployment model defines the purpose of the cloud and the nature of how the cloud is located. The NIST definition for the four deployment models is as follows [41]:

Public Cloud:A cloud infrastructure is provided to many customers and is managed by a third party [48]. 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 users pay for whatever they use. Examples of a public cloud include Microsoft Azure, Google App Engine.

Private Cloud:Cloud infrastructure, made available only to a specific customer and managed either by the organization itself or third party service provider [48]. This uses the concept of virtualization of machines, and is a proprietary network. One of the best examples of a private cloud is Eucalyptus Systems [7].

Community Cloud:Infrastructure shared by several organizations for a shared cause and may be managed by them or a third party service provider. An example of a Community Cloud includes Facebook

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.An example of a Hybrid Cloud includes Amazon Web Services (AWS).

Moreover, with the technological advancements, we can see derivative cloud deployment models emerging out of the various demands and the requirements of users. A similar example being a virtual-private cloud wherein a public cloud is used in a private manner, connected to the internal resources of the customer's data-centre [59]. With the emergence of high-end network access technologies like 2G, 3G, Wi-Fi, Wi-Max etc. and feature phones, a new derivative of cloud computing has emerged. This is popularly referred as ―Mobile Cloud Computing (MCC). It can be defined as a composition of mobile technology and cloud computing infrastructure where data and the related processing will happen in the cloud only with an exception that they can be accessed through a mobile device and hence termed as mobile cloud computing [24]. It's becoming a trend now-a-days and many organizations are keen to provide accessibility to their employees to access office network through a mobile device from anywhere. Recent technical advancements including the emergence of HTML5 and various other browser development

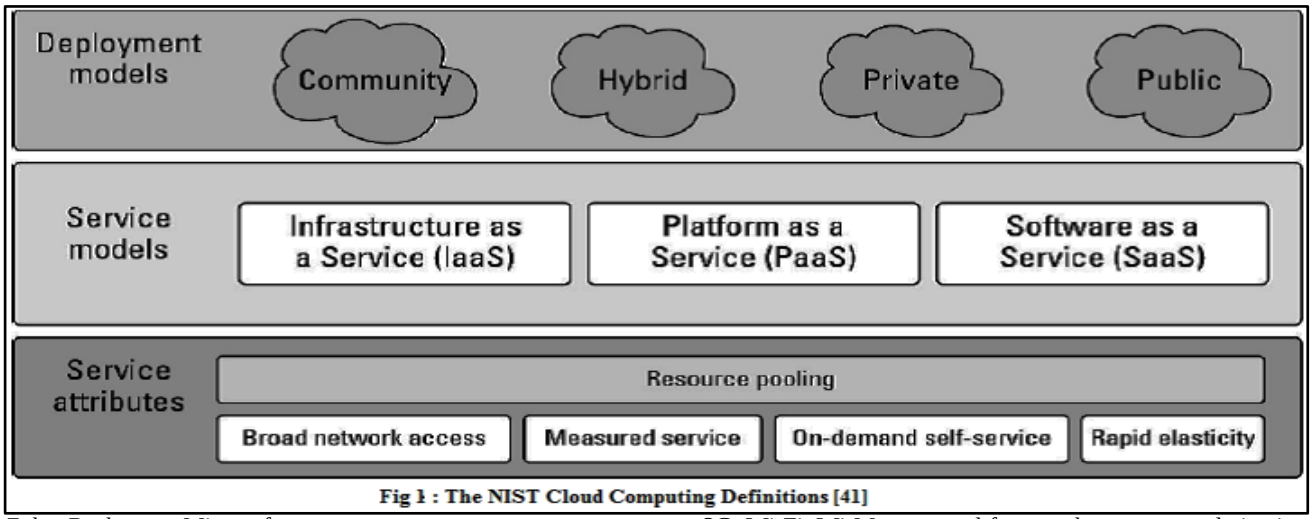

Fig 1 : The NIST Cloud Computing Definitions [41]

tools have only increased the market for mobile cloud-computing [37].

2.2 SERVICE MODELS

Cloud computing provides different services rather than a unit of product. According to the different types of services offered, cloud computing can be considered to consist of three layers: software as a service (SAAS), platform as a Service (PAAS), and infrastructure as a Service (IAAS) (Iyer and Henderson, 2010; Han, 2010, Mell and Grance, 2010). 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 [2, 25, 37].

Infrastructure-as-a-Serviceis the delivery of huge computing resources such as the capacity of processing, storage and network. Taking storage as an example, when a user use the storage service of cloud computing, he just pay the consuming part without buying any disks or even knowing nothing about the location of the data he deals with. Sometimes the IaaS is also called Hardware-as-a-Service (HaaS) [9, 34]. An example is Amazon Web Services

Platform-as-a-Servicegenerally abstracts the infrastructures and supports a set of application program interface to cloud applications. It is the middle bridge between hardware and application. Because of the importance of platform, many big companies want to grasp the chance of pre-dominating the platform of cloud computing as Microsoft does in personal computer time. The well-known examples are Google App Engine and Microsoft's Azure Services Platform.

Software-as-a-Serviceaims at replacing the applications running on PC. There is no need to install and run the special software on your computer if you use the SaaS. Instead of buying the software at a relative higher price, you just follow the pay-per-use pattern which can reduce you total cost. The concept of SaaS is attractive and some software runs well as cloud computing, but the delay of network is fatal to real time or half real time applications such as 3D online game. Salesforce.com offers this type of service.

3. PARAMETERS AFFECTING CLOUD SECURITY

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management [31].

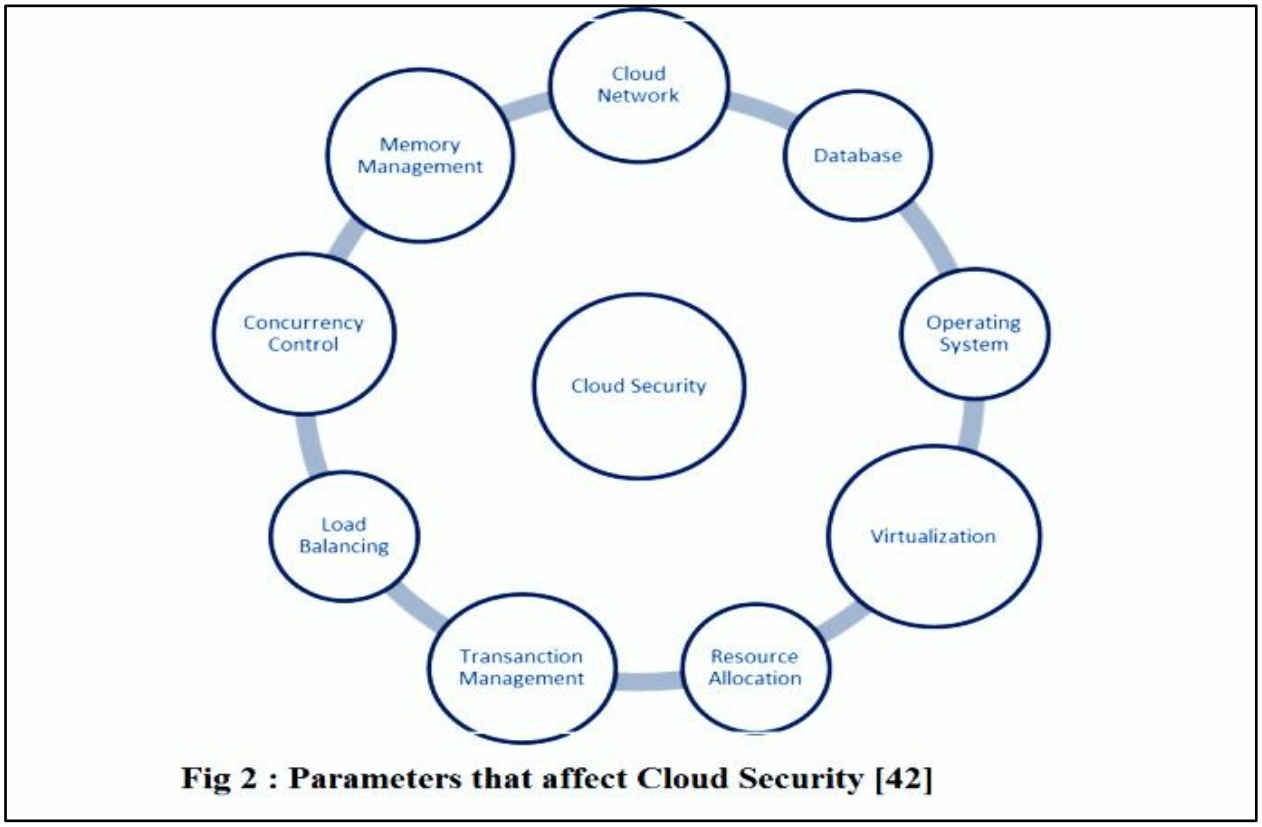

Fig 2 : Parameters that affect Cloud Security [42]

Security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

4. SECURITY ISSUES IN THE CLOUD DEPLOYMENT MODELS

In spite of being a buzzword, there are certain aspects associated with Cloud Computing as a result of which many organizations are still not confident about moving into the cloud. Certain loopholes in its architecture have made cloudcomputing vulnerable to various securities and privacy threats[47].Each of the three ways in which cloud services can

be deployed has its own advantages and limitations. And from the security perspective, all the three have got certain areas that need to be addressed with a specific strategy to avoid them.

4.1 Security Issues in a Public Cloud

In a public cloud, there exist many customers on a shared platform and infrastructure security is provided by the service provider. A few of the key security issues in a public cloud include[47]:

1) The three basic requirements of security: confidentiality, integrity and availability are required to protect data throughout its lifecycle. Data must be protected during the various stages of creation, sharing, archiving, processing etc. However, situations become more complicated in case of a public cloud where we do not have any control over the service provider's security practices [5].

2) In case of a public cloud, the same infrastructure is shared between multiple tenants and the chances of data leakage between these tenants are very high. However, most of the service providers run a multitenant infrastructure. Proper investigations at the time of choosing the service provider must be done in order to avoid any such risk [5, 45].

3) In case a Cloud Service Provider uses a third party vendor to provide its cloud services, it should be ensured what service level agreements they have in between as well as what are the contingency plans in case of the breakdown of the third party system.

4) Proper SLAs defining the security requirements such as what level of encryption data should undergo, when it is sent over the internet and what are the penalties in case the service provider fails to do so.

Although data is stored outside the confines of the client organization in a public cloud, we cannot deny the possibility of an insider attack originating from service provider's end. Moving the data to a cloud computing environment expands the circle of insiders to the service provider's staff and subcontractors [61]. An access control policy based on the inputs from the client and provider to prevent insider attacks has been proposed in [54]. Policy enforcement implemented at the nodes and the data-centres can prevent a system administrator from carrying out any malicious action. The three major steps to achieve this are: defining a policy, propagating the policy by means of a secure policy propagation module and enforcing it through a policy enforcement module.

4.2 Security Issues in a Private Cloud

A private cloud model enables the customer to have total control over the network and provides the flexibility to the customer to implement any traditional network perimeter security practice. Although the security architecture is more reliable in a private cloud, yet there are issues/risks that need to be considered [47]:

1) Virtualization techniques are quite popular in private clouds. In such a scenario, risks to the hypervisor should be carefully analysed. There have been instances when a guest operating system has been able to run processes on other guest VMs or host. In a virtual environment it may happen that virtual machines are able to communicate with all the VMs including the ones who they are not supposed to. To ensure that they only communicate with the ones which they are supposed to, proper authentication and encryption techniques such as IPsec [IP level Security] etc. should be implemented [58].

2) The host operating system should be free from any sort of malware threat and monitored to avoid any such risk [17]. In addition, guest virtual machines should not be able to communicate with the host operating system directly. There should be dedicated physical interfaces for communicating with the host.

3) In a private cloud, users are facilitated with an option to be able to manage portions of the cloud, and access to the infrastructure is provided through a webinterface or an HTTP end point. There are two ways of implementing a web-interface, either by writing a whole application stack or by using a standard applicative stack, to develop the web interface using common languages such as Java, PHP, Python etc. As part of screening process, Eucalyptus web interface has been found to have a bug, allowing any user to perform internal port scanning or HTTP requests through the management node which he should not be allowed to do. In the nutshell, interfaces need to be properly developed and standard web application security techniques need to be deployed to protect the diverse HTTP requests being performed [2].

4) While we talk of standard internet security, we also need to have a security policy in place to safeguard the system from the attacks originating within the organization. This vital point is missed out on most of the occasions, stress being mostly upon the internet security. Proper security guidelines across the various departments should exist and control should be implemented as per the requirements [17].

Thus we see that although private clouds are considered safer in comparison to public clouds, still they have multiple issues which if unattended may lead to major security loopholes.

The hybrid cloud model is a combination of both public and private cloud and hence the security issues discussed with respect to both are applicable in case of hybrid cloud. A trustmodel of cloud security in terms of social security has been discussed in [51]. Social insecurity has been classified as multiple stakeholder problem, open space security problem and mission critical data handling problem. All these issues have been considered while proposing a cloud trust model also known as "Security Aware Cloud". Two additional layers of trust: internal trust layer and contracted trust layer have been proposed to enhance security in a cloud computing environment.

5. SECURITY CONCERNS FOR CLOUD COMPUTING

While cost and ease of use are two great benefits of cloud computing, there are significant security concernsthat need to be addressed when considering moving critical applications and sensitive data to public and sharedcloud environments. These security concerns include both items that are related to traditional computing as well as security issues specific to cloud computing. Also, there are security issues that affect clients as well as providers. Most individuals think of attacks on the user's computer when computer security is mentioned. However, it is important to also consider that individuals can abuse cloud computing to create a virtual bot-network. To address these concerns, the cloud provider must develop sufficient controls to providethe same or a greater level of security than the organization would have if the cloud were not used.

5.1 CLOUD COMPUTING ATTACKS

As more companies move to cloud computing, look for hackers to follow. Some of the potential attack vectors criminals may attempt include [28, 47]:

A. DENIAL OF SERVICE:

When hackers overflows a network server or web server with frequent request of services to damage the network, the denial of service cannot keep up with them, server could not legitimate client regular requests. For example a hacker hijacks the web server that could stop the functionality of the web server from providing the services. In cloud computing, hacker attack on the server by sending thousands of requests to the server that server is unable to respond to the regular clients in this way server will not work properly. Counter measure for this attack is to reduce the privileges of the user that connected to a server. This will help to reduce the DOS attack. (Scarfone K, 2007).

B. SIDE CHANNEL ATTACKS:

An attacker could attempt to compromise the cloud by placing a malicious virtual machine in close proximity to a target cloud server and then launching a side channel attack.

C. AUTHENTICATION ATTACKS:

Authentication is a weak point in hosted and virtual services and is frequently targeted. There are many different ways to authenticate users; for example, based on what a person knows, has, or is. The Mechanisms used to secure the authentication process and the methods used are a frequent target of attackers.

D. MAN IN THE MIDDLE ATTACK:

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. Counter measure for this attack is SSL should properly install and it should check before communication with other authorized parties.

E. 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.

F. DNS ATTACKS:

A Domain Name Server (DNS) server performs the translation of a domain name to an IP address. Since the domain names are much easier to remember. Hence, the DNS servers are needed. But there are cases when having called the server by name, the user has been routed to some other evil cloud instead of the one he asked for and hence using IP address is not always feasible. Although using DNS security measures like: Domain Name System Security Extensions (DNSSEC) reduces the effects of DNS threats but still there are cases when these security measures prove to be inadequate when the path between a sender and a receiver gets rerouted through some evil connection. It may happen that even after all the DNS security measures are taken, still the route selected between the sender and receiver cause security problems [26].

G. 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. Counter measure for this attack is parties should useencryption methods for securing their data.

H. CROSS SITE SCRIPTING:

It is a type of attack in which user enters right URL of a website and hacker on the other site redirect the user to its own website and hack its credentials. For example user entered the URL in address bar and attacker redirects the user to hacker site and then he will obtain the sensitive data of the user. Cross site scripting attacks can provide the way to buffer overflows, DOS attacks and inserting spiteful software in to the web browsers for violation of user's credentials. (Yang, 2003)

I. 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. On the internet, IP space is associated in blocks and remains under the control of AS's. An autonomous system can broadcast information of an IP contained in its regime to all its neighbours. 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.

J. COOKIE POISONING:

It involves changing or modifying the contents of cookie to make unauthorized access to an application or to a webpage.Cookies basically contain the user's identity related credentials and once these cookies are accessible, the content of these cookies can be forged to impersonate an authorized user. This can be avoided either by performing regular cookie clean-up or implementing an encryption scheme for the cookie data [14].

K. HIDDEN FIELD MANIPULATION:

While accessing a web-page, there are certain fields that are hidden and contain the page related information and basically used by developers. However, these fields are highly prone to a hacker attack as they can be modified easily and posted on the web-page. This may result in severe security violations [25].

L. 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 backend 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 [64].

M. DISTRIBUTED DENIAL OF SERVICE ATTACKS:

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. 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 [50].

The DDoS attack is run by three functional units: A Master, A Slave and A Victim. Mater being the attack launcher is behind all these attacks causing DDoS, Slave is the network which acts like a launch pad for the Master. It provides the platform to the Master to launch the attack on the Victim. Hence it is also called as co-ordinated attack. Basically a DDoS attack is operational in two stages: the first one being Intrusion phase where the Master tries to compromise less important machines to support in flooding the more important one. The next one is installing DDoS tools and attacking the victim server or machine. Hence, a DDoS attack results in making the service unavailable to the authorized user similar to the way it is done in a DoS attack but different in the way it is launched. A similar case of Distributed Denial of Service attack was experienced with CNN news channel website leaving most of its users unable to access the site for a period of three hours [40]. In general, the approaches used to fight the DDoS attack involve extensive modification of the underlying network. These modifications often become costly for the users. [50] proposed a swarm based logic for guarding against the DDoS attack. This logic provides a transparent transport layer, through which the common protocols such as HTTP, SMTP, etc, can pass easily. The use of IDS in the virtual machine is proposed in [4] to protect the cloud from DDoS attacks. A SNORT like intrusion detection mechanism is loaded onto the virtual machine for sniffing all traffics, either incoming, or out-going. Another method commonly used to guard against DDoS is to have intrusion detection systems on all the physical machines which contain the user's virtual machines [10]. This scheme had been shown to perform reasonably well in a Eucalyptus [7] cloud.

N. CAPTCHA BREAKING:

CAPTCHA's were developed in order to prevent the usage of internet resources by bots or computers. They are used to prevent spam and overexploitation of network resources by bots. Even the multiple web-site registrations, dictionary attacks etc. by an automated program are prevented using a CAPTCHA. But recently, it has been found that the spammers are able to break the CAPTCHA [30], provided by the Hotmail and G-mail service providers. They make use of the audio system able to read the CAPTCHA characters for the visually impaired users and use speech to text conversion software to defeat the test. In yet another instant of CAPTCHA Breaking it was found that the net users are provided some form of motivation towards solving these CAPTCHA's by the automated systems and thus CAPTCHA Breaking takes place.

O. GOOGLE HACKING:

Google hacking refers to using Google search engine to find sensitive information that a hacker can use to his benefit while hacking a user's account.Generally, hackers try to find out the security loopholes by probing out on Google about the system they wish to hack and then after having gathered the necessary information, they carry out the hacking of the concerned system. In some cases, a hacker is not sure of the target. Instead he tries to Google out the target based on the loophole he wishes to hack a system upon. The hacker then searches all the possible systems with such a loophole and finds out those having the loopholes he wishes to hack upon. A Google hacking event was observed recently when login details of various g-mail users were stolen by a group of hackers in China. These had been some of the security threats that can be launched at the application level and cause a system downtime disabling the application access even to the authorized users.

P. PORT SCANNING:

There may be some issues regarding port scanning that could be used by an attacker as Port 80(HTTP) is always open that is used for providing the web services to the user. Other ports such as 21(FTP) etc. are not opened all the time it will open when needed therefore ports should be secured by encrypted until and unless the server software is configured properly. Counter measure for this attack is that firewall is used to secure the data from port attacks. (Services, 2009)

5.2 SECURITY THREATS PRESENT IN THE CLOUD AND THEIR MITIGATION

There are various security concerns that prevent customers from taking benefits of the cloud [3]. In this section, we have analyzed the security threats present in the cloud and their mitigation based on our experience of implementing the cloud.

A. VM-LEVEL ATTACKS:

The cloud computing is based on VM technology. For implementation of cloud, a hypervisor such as VMWare, vSphere, Microsoft Virtual PC, Xen etc. are used. This threat arises because of the vulnerabilities appearing in these hypervisors due to some facts being overlooked by developers during the coding of these hypervisors.

MITIGATION

The threat arising due to VM-Level vulnerabilities can be mitigated by monitoring through IDS (Instruction Detection System)/IPS (Intrusion Prevention System) and by implementing firewall.

B. ABUSE AND NEFARIOUS USE OF CLOUD COMPUTING:

This threat arises due to relatively weak registration systems present in the cloud computing environment. In cloud computing registration process, anyone having a valid credit card can register and use the service. This facilitates anonymity, due to which spammer, malicious code authors and criminals can attack the system.

MITIGATION

This type of threat can be mitigated in following ways:

- By implementing stricter registration process and validation process.
- By credit card fraud monitoring and coordination.
- Detailed introspection of user's network traffic.
- Network blocks through monitoring public black lists.

C. LOSS OF GOVERNANCE:

The client gives up control to the cloud provider on a number of issues while using the cloud infrastructure. The service Level Agreements (SLA) may not have commitment on the part of cloud provider, to provide such services, thus having a gap in security defences affecting security. This loss of control may lead to a lack of confidentiality, integrity and availability of data.

MITIGATION

There are no publicly available standards specific to cloud computing security. Thus organizations considering cloud services need to exercise persistent and careful efforts for the execution of Service Level Agreements (SLA).

D. XML SIGNATURE ELEMENT WRAPPING:

XML signature Element Wrapping is the fine renowned attack for web service. It is use to defend a component name, attribute and value from illegal party but unable to protect the position in the documents. (Jamil&Zaki, 2011b) Attacker

targets the component by operating the SOAP messages and putting anything that attacker like.

MITIGATION

Counter measure for this attack is using the digital certificate e.g. X.509 authorized by third party such as certificate authorities and also uses the mixture of WS-security with XML signature to a particular component. XML should have the list of components so that it can reject the messages which have malicious file and also reject theunexpected messages from the client.

E. BROWSER SECURITY:

As a client sent the request to the server by web browser the web browser have to make use of SSL (Secure Socket Layer) 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. (Jensen, 2009)

MITIGATION

Counter measure 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 (Simple Object Access Protocol) messages which does not have to be decrypted at mediator hosts.

F. CLOUD MALWARE INJECTION ATTACK:

The third issue is Cloud Malware Injection Attack, which tries to damage a spiteful service, application orvirtual 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.

MITIGATION

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.

G. FLOODING ATTACKS:

The fourth issue is Flooding Attack. Attacker attacks the cloud system openly. The most significant featureof cloud system is to make available of vigorously scalable recourses. Cloud system repeatedly increase its size when there is further requests from clients, cloud system initialize new service request in order to maintain client requirements. Flooding attack is basically distributing a great amount of non-sense requests to a certain service. Once the attacker throw a great amount of requests, by providing more recourses cloud system will attempt to work against the requests, ultimately system consume all recourses and not capable to supply service to normal requests from user. Then attacker attacks the service server. DOS attacks cost extra fees to the consumer for usage of recourses. In an unexpected situation the owner of the service has to compensate additional money.

MITIGATION

Counter measure for this attack is it's not easy to stop Dos Attacks. To stop from attacking the server, Intrusion detection system will filter the malicious requests, installing firewall. Occasionally intrusion detection system provides fake alerts and could mislead administrator.

H. LOCK-IN:

Lock-IN means inability of the customer to migrate from one cloud service provider to another .This is due to loss of portability of the customer data and programs. Presently, there are few tools, procedures or standard data formats which provide data, application or service portability. This prevents customers or organizations from adopting cloud computing.

MITIGATION

Standardized cloud Application Programming Interface (API) should be used. This standardization will ensure cloud computing to be more fully accepted.

I. INSECURE INTERFACES AND API'S:

Customers use a set of software Interfaces or APIs to interact with cloud services. The provisioning, management, orchestration and monitoring of the cloud service are generally done using these interfaces .If the weak set of interfaces and APIs are used, this may expose organizations to various security threats, such as anonymous access, reusable tokens or password, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring, and logging capabilities.

MITIGATION

To mitigate the above threats, the security model of cloud provider interfaces should be analyzed. Strong authentication and access controls should be implemented. Encryption should be used for transmission of content and, dependency chain associated with the API should be clearly understood.

J. ISOLATION FAILURE:

The services are delivered in cloud computing by sharing infrastructure .The components that are used to build Disk partitions, CPU cache, graphics processing units etc. are not designed to offer strong isolation properties or compartmentalization. The hypervisors, that are basic building blocks for cloud computing, have exhibited flaws that enable guest operating system to gain unauthorized control .Due to his isolation failure, the attackers focus on to impact the operations of other cloud customers to gain unauthorized access to data.

MITIGATION

Strong compartmentalization should be employed so that the individual customers do not impact the operations of other customers.This can be enforced by implementing best practices for installation, configuration, monitoring environment for unauthorized changes/activities, promoting strong authentication and access control, patching the vulnerabilities and conducting vulnerability scanning and configuration audits.

K. DATA LOSS OR LEAKAGE:

Data loss or leakages have an adverse effect on the business. The brand or reputation is completely lost and the customers' morale and trust are eroded. This data loss or leakage may be due to insufficient authentication, authorization and audit controls, inconsistent use of encryption and software keys, disposal challenges, a data centre reliability, and disaster recovery.

MITIGATION

The threats arising due to data loss or leakage can be mitigated by encrypting and protecting integrity of data in transit, analyzing data protection at both design and runtime,

implementing strong key generation, storage and management. Contractually demanding provider to wipe persistent media before it is released in to pool and contractually specifying provider backup and retention strategies.

L. ACCOUNT OR SERVICE HIJACKING:

The above threat occurs due to phishing, fraud and software vulnerabilities .Attackers can steal credentials and gain access to critical areas of deployed cloud computing services, resulting in compromise of the confidentiality, integrity and availability of these services.

MITIGATION

To mitigate the above threats, sharing of account credentials between users and services should not be allowed, multi-factor authentication techniques should be used wherever possible, strict monitoring should be done to detect unauthorized activity, and security policies, as well as SLAs of the cloud provider, should be clearly understood.

M. MANAGEMENT INTERFACE COMPROMISE

The customer management interface of the cloud provider is accessible through the internet .In cloud computing, larger set of resources are accessed through these interfaces than traditional hosting, since cloud computing provides remote access to customers through these management interfaces. This may pose a serious threat if web browser vulnerabilities are present.

MITIGATION

To mitigate threats arising due to remote access, secure protocol should be used to provide access. Also, web browser vulnerabilities should be completely patched before providing remote access.

N. COMPLIANCE RISKS:

This threat arises due to lack of governance over audits and industry standard assessments. Due to this, customers of cloud services do not have a view into the processes, procedures and practices of the provider in the areas of access, identity management and segregation of duties. Organizations that seek to obtain certification may be put at risk because cloud computing service providers may not be able to provide evidence of their own compliance with the necessary requirements or may not permit an audit by cloud customer.

MITIGATION

Vendors' internal audit process should be reviewed. How often it is audited by external agencies and, whether or not, it is open to being audited for compliance.

O. MALICIOUS INSIDERS:

This threat is well known to most organizations .Malicious insiders' impact on organization is considerable. Given their level of access, they can infiltrate organizations and assets and do brand damage, financial losses and productivity losses. Therefore, it is critical for customers of cloud services as to what controls have been provided by cloud providers to detect and defend against the malicious insider threats.

MITIGATION

The Malicious insider threats can be mitigated by specifying human resources requirements as part of legal contracts, conducting a comprehensive supplier assessment, providing transparency into overall information security and management practices, as well as compliance reporting and determining security breach notification processes.

6. SECURE CLOUD ARCHITECTURE

Cloud computing mostly involves deployment of virtualization technologies. Most organizations tend to deploy virtualization technologies by retrofitting their virtual networks with existing physical network. This is mainly due to non-involvement of information and network security teams in the initial planning stages. Due to this lack of technological preparedness, the network security weakens and this is a key factor to the success of cloud computing with large scale organizations [3]. We next, present cloud security architecture, using which, organizations can protect themselves against security threats and attacks. The key points for this architecture based on authors' analysis of existing

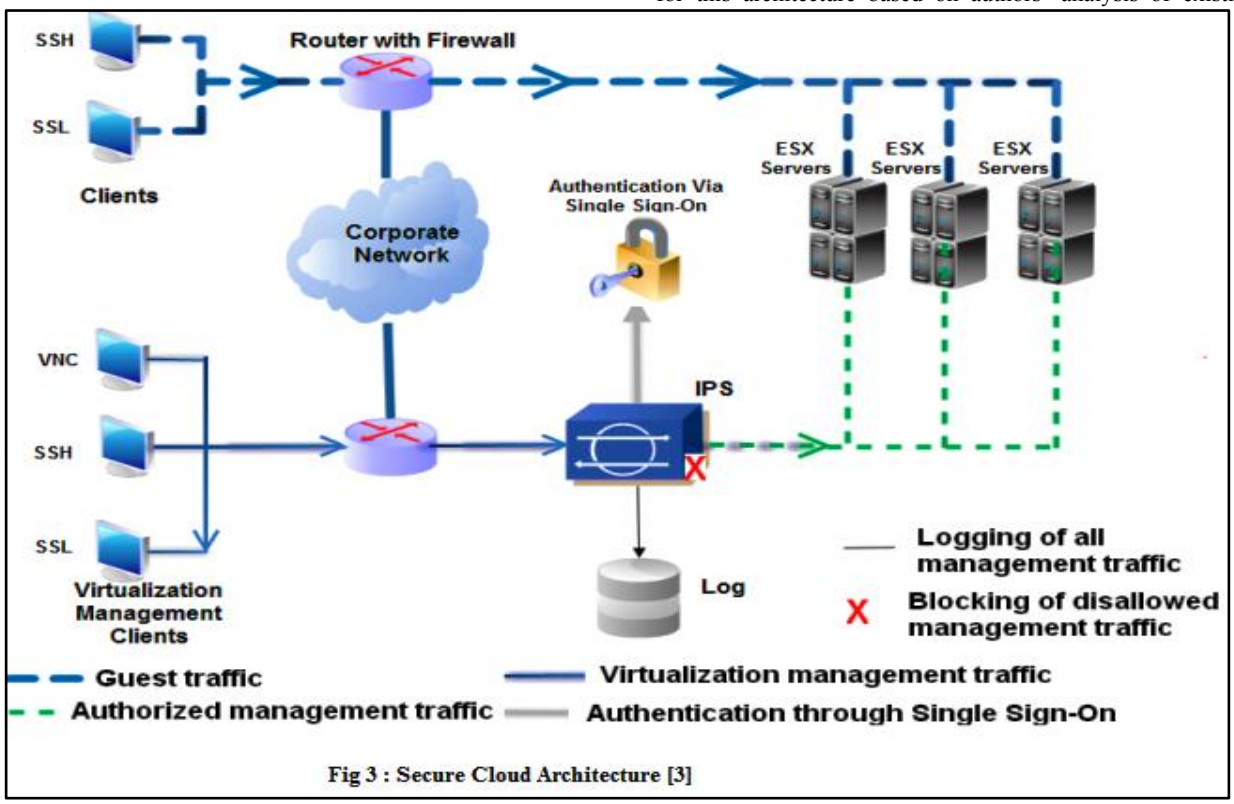

Fig 3 : Secure Cloud Architecture [3]

security technologies are:

A. Single Sign-On

In a cloud computing environment, workers log in to multiple applications and services. Due to this, it is very difficult to implement strong authentication at the user level. To overcome this problem, it is suggested that, to streamline security management and to implement strong authentication within the cloud, organizations should implement Single Sign-On for cloud users. This enables user to access multiple applications and services in the cloud computing environment through a single login, thus enabling strong authentication at the user level.

B. Increase Availability

Access to cloud service should be available all the time, even during maintenance. This makes critical business data stored in the cloud to be always available to cloud users, reducing network down time, thereby increasing business profits. This can be done by implementing high availability technologies such as active/active clustering, dynamic server load balancing and ISP load balancing within the network infrastructure.

C. Defence in Depth Approach

There should be a proper layered defence consisting of perimeter protection, and intrusion detection, and prevention components within the network. Virtual firewall appliances should be deployed instead of first-generation firewalls. This allows network administrators to inspect all levels of traffic, which includes basic web browser traffic, to peer-to-peer applications traffic and encrypted web traffic in the SSLtunnel.Intrusion Prevention Systems (IPS) should be installed to protect networks from internal threats from insiders.

D. Single Management Console

The Risk exponentially increases as additional network protection devices are deployed to protect the virtual network. This is due to human error involved, as deployment of more devices will increase the management consoles also. Hence, to overcome this problem, there should be single managementconsole to manage, monitor and configure all devices.

E. Virtual Machine Protection

Beneath every cloud implementation, there are virtual machines. These virtual machines are vulnerable like their physical counterparts. Hence, to adequately protect virtual machines, they should he isolated from other network segments and deep inspection at the network level should be implemented to prevent them both from internal and external threats. Illegal internal access should be restricted by implementing intrusion prevention systems and unauthorised external access should be protected by using secure remote access technologies like IPSec or SSL VPN. Based on above observations, secure cloud architecture has been physically implemented and is shown in Figure 3.

7. CONCLUSION

Cloud Computing, envisioned as the next generation architecture of IT Enterprise is a talk of the town these days. It is a new term introduced in business environment where users can interact directly with the virtualized resources and safe the cost for the consumers. The way cloud has been dominating the IT market, a major shift towards the cloud can be expected in the coming years. Cloud computing offers real benefits to companies seeking a competitive edge in today's economy. Many more providers are moving into this area, and the competition is driving prices even lower. Attractive pricing, the ability to free up staff for other duties, and the ability to pay for ―as needed services will continue to drive more businesses to consider cloud computing. Mobile cloud computing is expected to emerge as one of the biggest market for cloud service providers and cloud developers.

Although Cloud computing can be seen as a new phenomenon which is set to revolutionize theway we use the Internet, there is much to be cautious about. There are many new technologiesemerging at a rapid rate, each with technological advancements and with the potential of makinghuman's lives easier.Enterprises that are implementing cloud computing by expanding their on-premise infrastructure, should be aware of the security challenges faced by cloud computing. Cloud service providers need to inform their customers on the level of security that they provide on their cloud. Both the cloud service provider and the customer should make sure that the cloud is safe enough from all the external threats, so there will be a strong and mutual understanding between the customer and the cloud service provider. To protect against the compromise of the compliance integrity and security of their applications and data, a line of defence must be applied. This line of defence includes firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive enterprises and service providers should apply this protection on their cloud infrastructure, to achieve security so that they could take advantage of cloud computing ahead of their competitors. In order to keep the Cloud secure, these security threats need to be controlled. Moreover data residing in the cloud is also prone to a number of threats and various issues like confidentiality and integrity of data should be considered while buying storage services from a cloud service provider. Auditing of the cloud at regular intervals needs to be done to safeguard the cloud against external threats. In addition to this, cloud service providers must ensure that all the SLA's are met and human errors on their part should be minimized, enabling smooth functioning. This research effort presents an overview of Cloud Computing which includes different models of cloud computing and various security concerns related to the three basic services provided by a Cloud computing environment are considered and the solutions to prevent them have been discussed. Furthermore, a physical cloud computing security architecture has also been presented.

Cloud computing has the potential to become a frontrunner in promoting a secure, virtual and economically viable IT solution in the future. However, due to the complexity of the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be radically tweaked to be able to work with the clouds architecture As the development of cloud computing technology is still at an early stage, this research effort will provide a better understanding of the design challenges of cloud computing, and pave the way for further research in this area.

8. REFERENCES

[1] A Platform Computing Whitepaper. "Enterprise Cloud Computing: Transforming IT.", PlatformComputing, pp6, 2010.

[2] Alessandro Perilli, Claudio Criscione, "Securing the Private Cloud", Article on Secure Networks, Virtualization.info. http://virtualization.info/en/security/privatecloud.pdf

[3] AlokTripathy, Abhinav Mishra, "Cloud Computing Security Considerations", IEEE International Conference

on Signal Processing, Communications & Computing, Sept- 2011.

[4] AmanBakshi, Yogesh B. Dujodwala, "Securing cloud from DDoS Attacks using Intrusion Detection System inVirtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on CommunicationSoftware and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[5] A. Verma and S. Kaushal, "Cloud Computing Security Issues and Challenges: A Survey", Proceedings of Advances in Computing and Communications, Vol. 193, pp. 445-454, 2011.DOI: 10.1007/978-3-642-22726-4_46

[6] B.P. Rimal, Choi Eunmi, I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems", Intl. Joint Conference on INC, IMS and IDC, 2009, pp. 44-51,Seoul, Aug, 2009. DOI: 10.1109/NCM.2009.218

[7] B. R. Kandukuri, R. Paturi V, A. Rakshit, "Cloud Security Issues", In Proceedings of IEEE International Conference on Services Computing, pp. 517-520, 2009.

[8] Char Sample, Senior Scientist, BBN Technologies, Diana Kelley, Partner, Security Curve, "Cloud computing security: Routing and DNS security threats," http://searchsecurity.techtarget.com/tip/0, 289483, sid14_gci1359155_mem1, 00.html/.

[9] Cloud Computing. Wikipdia. Available at http://en.wikipedia.org/wiki/Cloud_computing

[10] ClaudioMazzariello, Roberto Bifulco and Roberto Canonico, "Integrating a Network IDS into an Open Source Cloud Computing Environment," Sixth International Conference on Information Assurance and Security, USA, pp. 265-270, Aug. 23-25, 2010. DOI: 10.1109/ISIAS.2010.5604069.

[11] Cong Wang, Qian Wang, KuiRen, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," 17th International workshop on Quality of Service, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4

[12] C. Weinhardt, A. Anandasivam, B. Blau, and J. Stosser."Business Models in the Service World."IT Professional, vol. 11, pp. 28-33, 2009.

[13] Daniel Oliveira and Eduardo Ogasawara. Article: Is Cloud Computing the Solution for Brazilian Researchers?. International Journal of Computer Applications 6(8):19–23, September 2010.

[14]D. Gollmann, "Securing Web Applications," Information Security Technical Report, vol. 13, issue. 1, 2008, Elsevier Advanced Technology Publications Oxford, UK, DOI: 10.1016/j.istr.2008.02.002.

[15] D. Oliveira, F. Baião, and M. Mattoso, 2010, "Towards Taxonomy for Cloud Computing from an e-Science Perspective", Cloud Computing: Principles, Systems and Applications (to be published), Heidelberg: Springer-Verlag.

[16] Dr.Gurdev Singh, ShanuSood, Amit Sharma, "CM-Measurement Facets for Cloud Performance", IJCA, , Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011.

[17] E. Mathisen, "Security Challenges and Solutions in Cloud Computing", Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp. 208-212, June, 2011, ISBN: 978-1-4577-0871-8, DOI: 10.1109/DEST.2011.5936627.

[18] Ertaul, L. and Singhal, S. 2009. Security Challenges in Cloud Computing. California State University, East Bay. Academic paper http://www.mcs.csueastbay.edu/~lertaul/Cloud%20Security%20CamREADY.pdf

[19] Gaoyun Chen, Jun Lu and Jian Huang, Zexu Wu, "SaaAS - The Mobile Agent based Service for Cloud Computing in Internet Environment", Sixth International Conference on Natural Computation, ICNC 2010, pp. 2935-2939, IEEE, Yantai, Shandong, China, 2010. ISBN: 978-1-4244-5958-2.

[20] Global Netoptex Incorporated. "Demystifying the cloud.Important opportunities, crucial choices." pp4-14. Available: http://www.gni.com [Dec. 13, 2009].

[21] Hanqian Wu, Yi Ding, Winer, C., Li Yao, "Network Security for Virtual Machines in Cloud Computing," 5th Int'l Conference on Computer Sciences and Convergence Information Technology, pp. 18-21, Seoul, Nov. 30- Dec. 2, 2010. ISBN: 978-1-4244-8567-3.

[22] Harjit Singh Lamba and Gurdev Singh, "Cloud Computing-Future Framework for emanagement of NGO's", IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[23] Harold C. Lin, ShivnathBabu, Jeffrey S. Chase, Sujay S. Parekh, "Automated Control in Cloud Computing: Opportunities and Challenges", Proc. of the 1st Workshop on Automated control for data centres and clouds, New York, NY, USA, pp. 13-18, 2009, ISBN: 978-1-60558-585-7.

[24] Hoang T. Dinh, Chonho Lee, DusitNiyato, Ping Wang, "A Survey of Mobile Cloud Computing: Architecture, Applications and Approaches", Wireless Communications and Mobile Computing, Wiley Inc.

[25] IanRathie, "An Approach to Application Security," White Paper, SANS Institute.

http://www.sans.org/reading_room/whitepapers/application/approach-application-security_16.

[26] I. Foster, Y. Zhao, I. Raicu, and S. Lu, 2008, Cloud Computing and Grid Computing 360-Degree Compared, In: Grid Computing Environments Workshop, 2008. GCE '08, p. 10, 1.

[27] Joachim Schaper, 2010, "Cloud Services", 4th IEEE International Conference on DEST, Germany.

[28] KausarFiazKhawaja, Sara Qaisar, "Cloud Computing: Network/Security Threats and Countermeasures", IJCRB, Vol. 3 No. 9, January 2012.

[29] K.Mukherjee and G.Sahoo. Article: Cloud Computing: Future Framework for e-Governance. International Journalof Computer Applications 7(7):31–34, October.

[30] K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection techniques for Grid and Cloud Computing Environment," IT Professional, IEEE Computer Society, vol. 12, issue 4, pp. 38-43, 2010.

[31] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, BhavaniThuraisingham, SecurityIssues for Cloud Computing, International Journal of Information Security and Privacy, 4(2),39-51, University of Texas, USA, April-June 2010.

[32] Kuyoro S.O., Ibikunle F., Awodele O., "Cloud Computing Security Issues & Challenges", IJCN, Vol. 3 Issue 5: 2011, pp. 247-255.

[33] Liladhar R Rewatkar and Ujwal A Lanjewar. Article: Implementation of Cloud Computing on Web Application. International Journal of Computer Applications 2(8):28–32, June 2010. Published By Foundation of Computer Science.

[34] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, 2009, A break in the clouds: towards a cloud definition, SIGCOMM Comput. Commun. Rev., v. 39, n. 1, p. 50-55

[35] L. Wang, GregorLaszewski, Marcel Kunze, Jie Tao, "Cloud Computing: A Perspective Study", New Generation Computing- Advances of Distributed Information Processing, pp. 137-146, vol. 28, no. 2, 2008. DOI: 10.1007/s00354-008-0081-5

[36] Meiko Jensen, JorgSchwenk, Nils Gruschka, Luigi Lo Iacon, "On technical Security Issues in Cloud Computing", Proc. of IEEE International Conference on Cloud Computing (CLOUD-II, 2009), pp. 109-116, India, 2009.

[37]Mohsin Nazir, "Cloud Computing: Overview & Current Research Challenges", IOSR-JCE, Vol. 8-No.1, Nov-Dec 2012, pp. 14-22.

[38] Muzafar Ahmad Bhat, RazeefMohd Shah, Bashir Ahmad and InayatRasoolBhat, "Cloud Computing: A Solution to Information Support Systems", IJCA, Vol. 11-No.5, December 2010, pp. 5-9.

[39] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. "What's Inside the Cloud? An Architectural Map of the Cloud Landscape."IEEEXplore, pp 23-31, Jun. 2009.

[40]Nathan Mcfeters, "Recent CNN Distributed Denial of Service Attack Explained". http://www.zdnet.com/blog/security/recent-cnn-distributed-denial-of-service-ddos-attack-explained/1054.

[41] Peter Mell, Timothy Grance, "The NIST Definition of Cloud Computing", Jan, 2011. http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf

[42] Prince Jain, "Security Issues & their solution in Cloud Computing", International Journal of Computing & Business Research.

[43] Pring et al., "Forecast: Sizing the cloud; understanding the opportunities in cloud services," Gartner Inc., Tech. Rep. G00166525, March 2009.

[44] Problems Faced by Cloud Computing, Lord CrusAd3r,dl.packetstormsecurity.net/.../ProblemsFacedbyCloudComputing.pdf.

[45] P. Sharma, S. K. Sood, and S. Kaur, "Security Issues in

Cloud Computing", Proceedings of High Performance

Architecture and Grid Computing, Vol. 169, pp. 36-45, 2011.DOI: 10.1007/978-3-642-22577-2_5

[46] Rabi Prasad Padhy, ManasRajanPatra and Suresh Chandra Satapathy, "Cloud Computing: Security Issues & Research Challenges", IJCSITS, Vol. 1-No.2, December 2011, pp. 136-146.

[47] RohitBhadauria, SugataSanyal, "Survey on Security Issues in Cloud Computing & Associated Mitigation Techniques", IJCA, Vol. 47-No. 18, June 2012, pp. 47-66.

[48] R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2), pp. 23-27, 2009, ISSN: 1520-9202.

[49] R. Maggiani, Communication Consultant, Solari Communication, "Cloud Computing is Changing How we Communicate", 2009 IEEE International Professional Conference, IPCC, pp. 1-4, Waikiki, HI, USA, July 19-22, 2009. ISBN: 978-1-4244-4357-4.

[50] RuipingLua and Kin Choong Yow, "Mitigating DDoS Attacks with Transparent and Intelligent Fast-Flux Swarm Network," IEEE Network, vol. 25, no. 4, pp. 28-33, July-August, 2011.

[51] Sato, H; Kanai, A; Tanimoto, S; "A Cloud Trust Model in a Security Aware Cloud", Intl. Symposium on Applications and the Internet (SAINT), pp. 121-124, July, 2010, Seoul.

[52] SangeetaSen, RituparnaChaki, "Handling Write Lock Assignment in Cloud Computing Environment", Communications in Computer and Information Science, vol. 245, issue. 7, pp. 221-230, 2011. DOI: 10.1007/978-3-642-27245-5_27

[53] SonalAnand, Sarvesh Gupta, ShwetaFatnani, Varsha Sharma and Deepti Jain. Article: Semantic Cloud for Mobile Technology. International Journal of Computer Applications 8(12):1–4, October 2010.

[54] SudharsanSundararajan, Hari Narayanan, Vipin Pavithran, KaladharVorungati, KrishnashreeAchuthan, "Preventing Insider attacks in the Cloud", Communications in Computer and Information Science, vol. 190, issue. 5, pp. 488-500, 2011.DOI: 10.1007/978-3-642-22709-7_48

[55] Sun Microsystems White Paper, ―Introduction to Cloud Computing Architecture,‖ June 2009.

[56] S. Arnold (2009, Jul.). "Cloud computing and the issue of privacy."KM World, pp14-22. Available: www.kmworld.com [Aug. 19, 2009].

[57] S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing"; Journal of Network and Computer Applications, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, 2011, ISSN: 1084-8045.

[58] Thomas W. Shinder, "Security Issues in CloudDeployment models", TechNet Articles, Wiki,Microsoft, Aug, 2011.

http://social.technet.microsoft.com/wiki/contents/articles/security-issues-in-cloud-deployment-models.aspx

[59] Timothy Wood, PrashantShenoy, Alexandre Gerber, K.K. Ramkrishnan, Jacobus Van der Merwe, "The Case for Enterprise-Ready Virtual Private Clouds", HotCloud'09 Proceedings of the 2009 conference on Hot topics in cloud computing, San Diego, CA, USA, 2009. http://www.usenix.org/event/hotcloud09/tech/full_papers/wood.pdf

[60] V. Krishna Reddy, B. ThirumalRao, Dr. L.S.S. Reddy, P.SaiKiran "Research Issues in Cloud Computing " Global Journal of Computer Science and Technology, Volume 11, Issue 11, July 2011.

[61] Wayne Jansen, Timothy Grance, "NIST Guidelines on Security and Privacy in Public Cloud Computing", Draft Special Publication 800-144, 2011. http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf.

[62] W.K. Chan, Lijun Mei, and Zhenyu Zhang, "Modeling and testing of cloud applications", to appear in Proceedings of 2009 IEEE Asia-Pacific Services Computing Conference (APSCC 2009), (Singapore, December 7-11, 2009), IEEE Computer Society Press, Los Alamitos, CA, USA, 2009.

[63] X. Zhang, N. Wuwong, H. Li, and X. J. Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments", In Proceedings of 10th IEEE International Conference on Computer and Information Technology, pp. 1328- 1334, 2010.

[64] ZouheirTrabelsi, HamzaRahmani, KamelKaouech, MounirFrikha, "Malicious Sniffing System Detection Platform", Proceedings of the 2004 International Symposium on Applications and the Internet, pp. 201-207, 2004, ISBN: 0-7695-2068-5.