TOP THREATS TO CLOUD COMPUTING SECURITY

Muhammad Adeel Javaid
Member Vendor Advisory Council CompTIA

Abstract:

Cloud computing is a growing area of concern in the IT security community because cloud architectures are literally popping up all over. Public clouds are available from Google.com, Amazon.com, Microsoft, Oracle/Sun, Canonical/Eucalyptus and many other vendors. Private cloud technologies, where the cloud software is loaded on local or in-house server hardware, are available from VMware, Eucalyptus, Citrix, Microsoft, and there are thousands of vendors offering cloud solutions of all sorts. A search for private cloud hosting on Google.com produced 581,000 page results.

Strong cloud security begins with the infrastructure. If the cloud system's infrastructure is insecure, it puts the confidentiality and availability of all information used via that cloud system at risk. The infrastructure constitutes a cloud system's first line of defense. This can be enforced by patching servers, configuring firewalls, and placing intrusion- detection systems (IDS). Security Pain Points must be identified.

This paper is concerned with discovery of the vulnerabilities in the landscape of clouds, discovery of security solutions, and finding evidence that early-adopters or developers have grown more concerned with security.

Key words: cloud security, secure cloud, cloud computing threats, cloud computing security

What is Cloud Computing?

Cloud computing is a convenient, on-demand model for network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The cloud element of cloud-computing derives from a metaphor used for the Internet, from the way it is often depicted in computer network diagrams. Conceptually it refers to a model of scalable, real-time, internet-based information technology services and resources, satisfying the computing needs of users, without the users incurring the costs of maintaining the underlying infrastructure. Examples in the private sector involve providing common business applications online, which are accessed from a web browser, with software and data stored on the "cloud" provider's servers.

Cloud Computing Convenience and Capability

Capability is about the ability to do things that otherwise couldn't be done. A great appeal of the cloud is the potential to create new solutions that were not technically or economically feasible without the use of cloud services. A key example is new application development. One of the main characteristics of cloud computing that enables these capabilities is elasticity.

Additional potential for cloud use is to enable federal employees to work in real time from remote locations, reducing travel costs and energy consumption, and improving the Government's emergency preparedness capabilities. Cloud-computing and "work-at-a-distance" represent major new Government-wide initiatives, supported by the CIO Council under the auspices of the Federal CIO and funded through the General Services Administration (GSA) as the service-provider.

Essential Characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and personal digital assistants (PDAs)).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the subscriber generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models:

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Who are the Major Service Providers?

The cloud is a shared and largely virtual environment, Data owners need to understand the implications of their data residing in the cloud service provider's data center and under its protection. It's critical that a user or an agency understands the controls its cloud provider has in place. In the cloud, federal managers need to recognize that while they still retain accountability for their data, the responsibility for its protection has passed to the vendor.

Understanding how the service provider has historically gone to market within the federal environment may be an indication of who to select when the agency is ready to decide on a vendor. Large -scale cloud providers are expected to be more secure than smaller or less established companies out there offering cloud services, because they have the experienced personnel, resources, and infrastructure that smaller organizations might lack.

The list of cloud computing solutions and service providers continues to grow daily. The sample given in Table 1 is illustrative and does not imply any federal endorsement.

Software as a Service (Saas)		Platform as a Service	
• Google Apps • Zoho Office • Workday • Microsoft Office Live	• Oracle On Demand Apps • NetSuite ERP • Salesforce.com SFA	• Amazon E2C • Salesforce.com Force.com • Google App Engine	• Coghead • Etelos • LongJump • Boomi • Microsoft Azure
External IaaS		**Internal IaaS**	
• HP/EDS (TBD) • IBM Blue Cloud • Sun Grid	• Joyent • Rackspace • Jamcracker	• HP Adaptive Infrastructure as a Service	
Utility Systems Management Tools+		**Utility Application Development**	
• VMWare • IBM Tivoli • Cassatt • Parallels	• Xen • Zuora • Aria Systems • eVapt	• Data Synapse • Univa UD • Elastra Cloud Server • 3tera App Logic	• IBM WebSphere XD • BEA Weblogic Server VE • Mule

Table 1: The list of cloud computing solutions and service providers

Threat Model for Cloud:

An abstract view of threat model for Cloud computing is shown in the Figure 1 below. Cloud clients are facing two types of security threats viz; external and internal attacks.

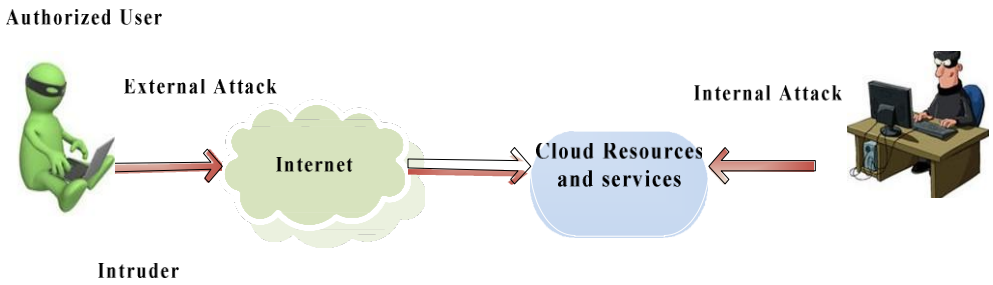

Figure 1: An abstract view of threat model for Cloud computing

External network attacks in the cloud are increasing at a notable rate. Malicious user outside the Cloud often performs DoS or DDoS attacks to affect the availability of Cloud services and resources. Port scanning, IP spoofing, DNS poisoning, phishing are also executed to gain access of Cloud resources. A malicious user can capture and analyze the data in the packets sent over this network by packet sniffing. IP spoofing occurs when a malicious user impersonates a legitimate users IP address where they could access information that they would not have been able to access otherwise. Availability is very important. Not having access to services when needed can be a disaster for anyone especially in the case of being denied service. This can occur when exhaustion of the host servers causes requests from legitimate consumers to be denied. This can cost a company large amounts of money and time if the services they depend on to operate are not available.

Internal attacker (authorized user) can easily get access to other user's resources without being detected. An insider has higher privileges and knowledge (related to network, security mechanism and resources to attack) than the external attacker. Therefore, it is easy for an insider to penetrate an attack than external attackers.

Vulnerabilities:

In Cloud, existing vulnerabilities, threats, and associated attacks raise several security concerns. Vulnerabilities in Cloud can be defined as the loopholes in the security architecture of Cloud, which can be exploited by an adversary via sophisticated techniques to gain access to the network and other infrastructure resources. In this section, we discuss major Cloud specific vulnerabilities, which pose serious threats to Cloud computing.

Session Riding and Hijacking:

Session hijacking refers to use of a valid session key to gain unauthorized access for the information or services residing on a computer system, it also refers to theft of a cookie used to authenticate a user to a remote server and it is relevant to web application technologies weaknesses in the web application structure at their disposal that gives the chance to hackers in order to accomplish a wide variety of malicious activities. While session riding refers to the hackers sending commands to a web application on behalf of the targeted user by just sending that user an email or tricking the user into visiting a specially crafted website. Session riding deletes user data, executes online transactions like bids or orders, sends spam to an intranet system via internet and changes system as well as network configurations or even

opens the firewall. However, the web technologies evolution and refinement also brings new techniques that compromise sensitive data, provide access to theoretically secure networks and pose threats to the daily operation of online businesses.

Reliability and Availability of Service:

In terms of reliability and availability, cloud computing is not a perfect technology. For example in February 2008, Amazon's Web Service (Amazons-S3) cloud storage infrastructure went down for several hours, causing data loss and access issues with multiple Web 2.0 services. With more services being built on top of cloud computing infrastructures, an outage or failure can create a domino effect by taking down large amounts of Internet based services and applications which raise several questions such as in cases of failure, what forms of settlement exist for stakeholders? What is the responsibility of cloud providers? What will be appropriate procedures to overcome these issues?

Insecure Cryptography:

Attackers' can decode any cryptographic mechanism or algorithm as main methods to hack them are discovered. It's common to find crucial flaws in cryptographic algorithm implementations, which can twist strong encryption into weak encryption or sometimes no encryption at all. For example in cloud virtualization providers uses virtualization software to partition servers into images that are provided to the users as on-demand services. Although utilization of those VMs into cloud providers' data centres provides more flexible and efficient setup than traditional servers but they don't have enough access to generate random numbers needed to properly encrypt data. This is one of the fundamental problems of cryptography. How do computers produce truly random numbers that can't be guessed or replicated? In PCs, OS typically monitors users' mouse movements and key strokes to gather random bits of data that are collected in a so-called Entropy Pool (a set of unpredictable numbers that encryption software automatically pulls to generate random encryption passkeys). In servers, one that don't have access to a keyboard or mouse, random numbers are also pulled from the unpredictable movements of the computer's hard drive. VMs that act as physical machines but are simulated with software have fewer sources of entropy. For example Linux-based VMs, gather random numbers only from the exact millisecond time on their internal clocks and that is not enough to generate strong keys for encryption.

Data Protection and Portability:

Although the cloud services are offered based on a contract among client and a provider but what will happen when the contract is terminated and client doesn't wants to continue anymore. The question is, will the sensitive data of client be deleted or misused by the provider. Secondly if the provider went out of business due to any reason, what will happen to the services and data of the client? Will the provider handout the data of client to some other provider, if yes, will client trust the new provider? Considering these questions we can say that data protection and portability remains as one of main weaknesses of cloud computing.

Attacks on Cloud Computing

By exploiting vulnerabilities in Cloud, an adversary can launch the following attacks.

Zombie Attack:

Through the Internet, an attacker tries to flood the victim by sending requests from innocent hosts in the network. These types of hosts are called *zombies*. In the Cloud, the requests for Virtual Machines (VMs) are accessible by each user through the Internet. An attacker can flood the large number of requests via *zombies*. Such an attack interrupts the expected behavior of Cloud affecting availability of Cloud services. The Cloud may be overloaded to serve a number of requests, and hence exhausted, which can cause DoS (Denial of Service) or DDoS (distributed denial of service) to the servers. Cloud in the presence of attacker's flooded requests cannot serve valid user's requests.

Mitigation: However, better authentication and authorization and IDS/IPS can provide protection against such an attack.

Service Injection Attack:

Cloud system is responsible for determining and eventually instantiating a free-to- use instance of the requested service. The address for accessing that new instance is to be communicated back to the requesting user. An adversary tries to inject a malicious service or new virtual machine into the Cloud system and can provide malicious service to users. Cloud malware affects the Cloud services by changing (or blocking) Cloud functionalities. Consider a case wherein an adversary creates his/her malicious services like SaaS, PaaS, or IaaS and adds it to the Cloud system. If an adversary succeeds to do this, then valid requests are redirected to the malicious services automatically.

Mitigation: To defend against this type of attack, service integrity checking module should be implemented. Strong isolation between VMs may disable the attacker from injecting malicious code in the neighbor's VM.

VM Escape:

In this type of attack, an attacker's program running in a VM breaks the isolation layer in order to run with the hypervisor's root privileges instead with the VM privileges. This allows an attacker to interact directly with the hypervisor. Therefore, VM Escape from the isolation is provided by the virtual layer. By VM Escape, an attacker gets access to the host OS and the other VMs running on the physical machine.

Rootkit in Hypervisor:

VM-based rootkits initiate a hypervisor compromising the existing host OS to a VM. The new guest OS assumes that it is running as the host OS with the corresponding control over the resources, however, in reality this host does not exist. Hypervisor also creates a covert channel to execute unauthorized code into the system. This allows an attacker to control over any VM running on the host machine and to manipulate the activities on the system.

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.

Man in the Middle Attack:

If secure socket layer (SSL) is not properly configured, then any attacker is able to access the data exchange between two parties. In Cloud, an attacker is able to access the data communication among data centers.

Mitigation: Proper SSL configuration and data communication tests between authorized parties can be useful to reduce the risk of Man-in-the-Middle attack.

Metadata Spoofing Attack:

In this type of attack, an adversary modifies or changes the service's Web Services Description Language (WSDL) file where descriptions about service instances are stored. If the adversary succeeds to interrupt service invocation code from WSDL file at delivering time, then this attack can be possible.

Mitigation: To overcome such an attack, information about services and applications should be kept in encrypted form. Strong authentication (and authorization) should be enforced for accessing such critical in- formation.

Phishing Attack:

Phishing attacks are well known for manipulating a web link and redirecting a user to a false link to get sensitive data. In Cloud, it may be possible that an attacker use the cloud service to host a phishing attack site to hijack accounts and services of other users in the Cloud.

Backdoor Channel Attack:

It is a passive attack, which allows hackers to gain remote access to the compromised system. Using backdoor channels, hackers can be able to control victim's resources and can make it a *zombie* for attempting a DDoS attack. It can also be used to disclose the confidential data of the victim.

Mitigation: Better authentication and isolation between VMs can provide protection against such attacks.

Secure Cloud Architecture

Here is a cloud security architecture, which protect organization against security threats and attacks. The key points for this architecture based on our analysis of existing security technologies are:

Single Sign-on:

Currently, Users are having multiple accounts in various Service Providers with different usernames accompanied by different password. Therefore the vast majority of network users tend to use the same password wherever possible, posing inherent security risks.The inconvenience of multiple authentications not only causes users to lose productivity, but also imposes more administrative overhead. Enterprises today are seriously considering the use of Single Sign On (SSO) technology to address the password explosion because they promise to cut down multiple network and application passwords to one.

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.

Defence in Depth Security Approach:

As enterprise networking technology has evolved, so too has enterprise security. What began simply as setting up a perimeter around the network via fairly basic security tools like firewalls and email gateways, has evolved into adding an array of virtual private networks (VPNs), virtual local area network (VLAN) segmentation, authentication, and intrusion detection systems (IDS) necessary to handle the consistently growing number of threats to the corporate 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 SSL tunnel .Intrusion Prevention Systems (IPS) should be installed to protect networks from internal threats from insiders.

Increase Availability:

Availability is a reoccurring and a growing concern in software intensive systems. Cloud systems services can be turned offline due to conservation, power outages or possible denial of service invasions. Fundamentally, its role is to determine the time that the system is up and running correctly; the length of time between failures and the length of time needed to resume operation after a failure. Availability needs to be analyzed through the use of presence information, forecasting usage patterns and dynamic resource scaling. 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 balanced and ISP load balancing within the network infrastructure.

Data Privacy:

Cloud data privacy problem will be found at every stage of the life cycle. For the data storage and use, Mow bray et al. proposed a client-based privacy management tool that provides a user-centric trust model to help users control their sensitive information during the cloud storage and use.

Data loss prevention (DLP) tools as illustrated in Figure 2 can help control migration of data to the cloud and also find sensitive data leaked to the cloud. Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside of the corporate network. DLP help a network administrator control what data end users can transfer.

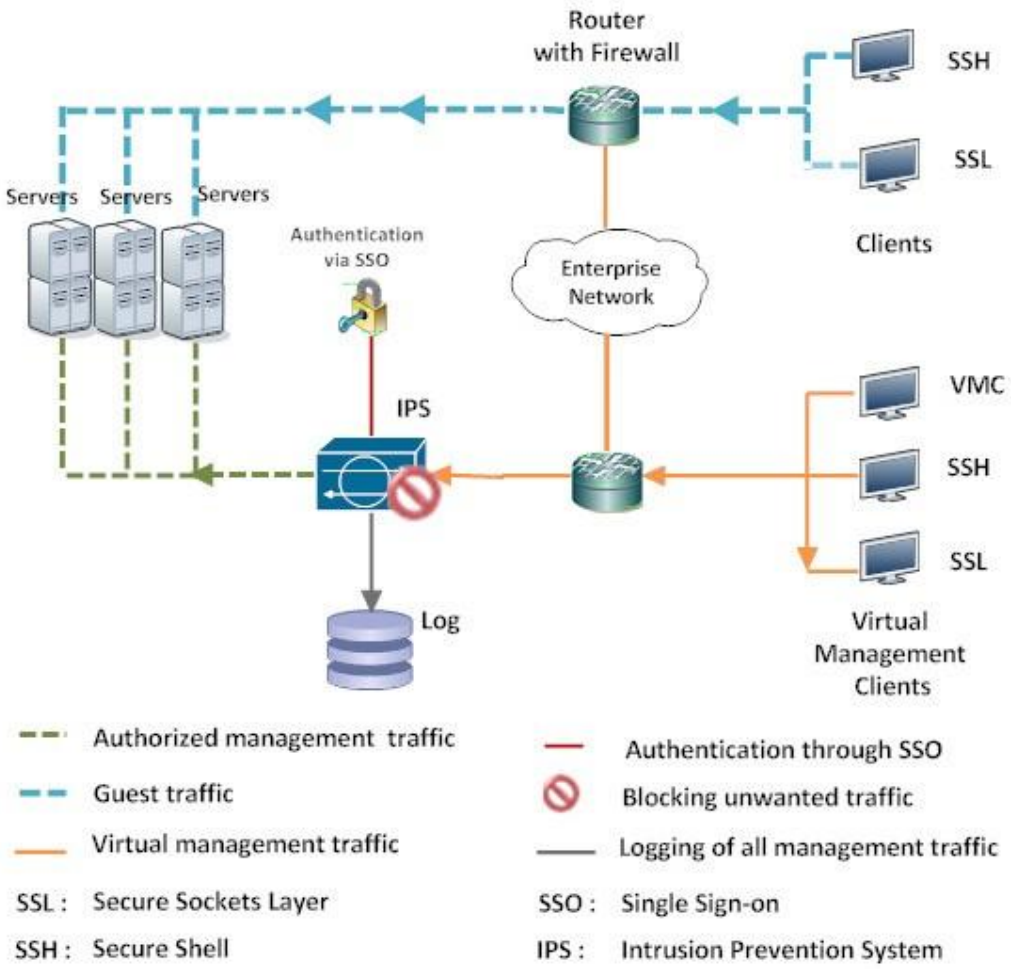

Figure 2: Data loss prevention (DLP) tools

Data Integrity:

As a result of large scale data communication cost, the users don't want to download data but verify its correctness. Therefore, users need to retrieve the little cloud data through some kinds of agreements or

knowledge's which are the probability of analytical tools with high confidence level to determine whether the remote data integrity. User can do the increase and decrease of the data capacity in the cloud server with the help of CSP(cloud service provider) in his request. This storage level must be with flexible and durability condition as far as its entire design or structure is concerned. Thus it should be claimed extra storage space concerning future process in data exchange.

Virtual Machine Protection:

You can't just install your firewall or antivirus software on a cloud-based virtual machine. Physical firewalls aren't designed to inspect and filter the vast amount of traffic originating from a hypervisor running 10 virtualized servers. Because VMs can start, stop and move from hypervisor to hypervisor at the click of a button, whatever protection you've chosen has to handle these activities with ease. Plus, as the number of VMs increases in the data center, it becomes harder to account for, manage and protect them. And if unauthorized people gain access to the hypervisor, they can take advantage of the lack of controls and modify all the VMs housed there.

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 unauthorized external access should be protected by using secure remote access technologies like IPSec or SSL VPN.

Conclusion

In this paper we have discussed the characteristics of a cloud security that contains threats/attacks and vulnerabilities. Organizations that are implementing cloud computing by expanding their on-premise infrastructure, should be aware of the security challenges faced by cloud computing. To protect against the compromise of the compliance integrity and security of their applications and data, defense in depth approach must be applied. This line of defense includes firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive organizations 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 this paper, a physical cloud computing security architecture has been presented. In future, the proposed architecture may be modified with the advancement of security technologies used for implementing this physical cloud security architecture. By considering the contributions from several IT industries worldwide, it's obvious that cloud computing will be one of the leading strategic and innovative technologies in the near future.

References

I- "Swamp Computing" a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010- 01-25.

II- "Thunderclouds: Managing SOA-Cloud Risk", Philip Wik". Service Technology Magazine. 2011-10. Retrieved 2011-21-21.

III- Ponemon (2011) Security of cloud computing providers study. http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf

IV- Tripathi and A. Mishra, "Cloud computing security considerations" IEEE Int. conference on signalprocessing, communication and computing (ICSPCC), 14-16 Sept., Xi'an, Shaanxi, China, 2011

V- Vadym Mukhin, Artem Volokyta, "Security Risk Analysis for Cloud Computing Systems" The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Prague, Czech Republic, 15-17 September 2011

VI- Meiko Jensen ,Jorg Sehwenk et al., “On Technical Security,Issues icloud Computing ”IEEE International conference on cloud Computing, 2009.

VII- M.Jensen ,N.Gruschka et al., “The impact of flooding Attacks on network based services”Proceedings of the IEEE International conference on Availiabilty,Reliability and Security (ARES) 2008.

VIII- Wayne A. Jansen, _Cloud Hooks: Security and Privacy Issues in Cloud Computing_, 44th Hawaii International Conference on System Sciesnces 2011.

IX- B. Grobauer, T. Walloschek, and E. Stocker, “Understanding Cloud Computing Vulnerabilities,” Security & Privacy, IEEE, vol. 9, no. 2, pp.50-57, 2011.

X- security-technology-cionetwork- cloud-computing.html, 2009, [Accessed: 20-Jul-2011].