International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 3, Issue 4, July-August 2014 **ISSN 2278-6856**

Cloud threat and security concern

Shreya Mishra
Dehradun Institute of Technology University
Mussourie-Diversion Road, Dehradun, Uttarakhand-248009,India

Abstract

Cloud computing is an alternative delivery and acquisition model for IT-related services. This Paradigm will shift the way purchasers of IT products and services contract with vendors and the way those vendors deliver their products. However, there are also risks and obstacles that evolve from this model. In this paper we shall discuss security concerns and various threats in Cloud Computing. This paper also presents some security area related to application security, data center operations, DP/BCP, security of hypervisors etc.

Keywords:- Authentication attack ,DDos attack, hypervisor ,Malware injection attack, ,side channel attack, virtualization, etc.

1. INTRODUCTION

One common complain among traveling employees is that their security software and policy slips out of date while they work away from the office. When they return, their non-compliant systems are blocked from accessing the network, and all productive activities comes to an end while their computers download security updates and apply the latest policy. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). Cloud computing is a disruptive technology (i.e. it creates a new market and technology that brings traditional system to a halt that has the potential to enhance collaboration, agility, scaling, and availability, flexibility and provides very optimum of efficient computing and causes a that are most pertinent to IT organizations and might cause some deterioration in clouds performance.

Cloud computing security

also called as "cloud security" is an evolving sub-domain of computer security, network security, information security. It includes many policies, specification, and controls that are imposed by third party i.e. cloud service provider to preserve CIA's(confidentiality, integrity and availability),to protect network from misuse, modification and to prevent unauthorized access. Cloud have various service models like Saas(Software-as-a-service),PaaS(Platform-as-a-Service);IaaS(Infrastructure-as-aService) and deployment model like Private cloud, public cloud, community cloud, hybrid cloud. There are many security issues in cloud as it circumscribe many technologies including Networks, databases, concurrency management, memory management operating systems, resource scheduling, transaction management, load balancing and most important virtualization.

2. VARIOUS TYPE OF ATTACKS POSSIBLE IN CLOUD

2.1 Denial of Service (DoS) attacks and Distributed DoS (ddos)-Denial-Of-Service *attack* is a attack on availability. In DoS attack, an unauthorized user sent fake request to the server that consumes all the bandwidth that prevents the authorized user to get access. Cloud System, is prone to Distributed Denial Of Service attack(DDoS).DDoS increases the number of packets per second and bits in transmission per second that causes traffic and consumes all bandwidth. In a cloud system, all the computational servers work in a service specific manner, with internal communication between them. The efficiency of cloud to process requests effectively is achieved by property of load balancing. As shown in Figure-1 whenever any server reached its threshold value i.e. overloaded then it transfers some of its jobs to a nearest and similar service-specific server to offload itself. An opponent must be authorized to get service from cloud. After being authorized the opponent can create some spurious data and pose the request to server. While processing these requests, the server first checks the authenticity of the requested jobs. Because only legitimate user can get access, so the authencity check would consumes CPU cycles, memory and engages the IaaS largely. This type of attack is also called Flooding Attack.

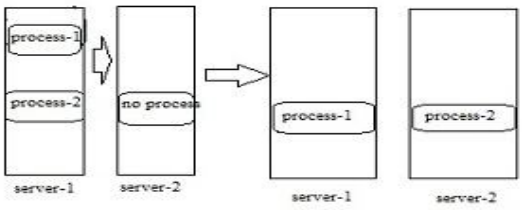

Figure-1:Load Balancing Process Of Cloud Server

Hence, DoS attacks do not wish to modify data or gain illegal access, but instead they target to crash the servers and whole networks. DoS attacks can be launched from either a single source or multiple sources. Multiple source DoS attacks are called distributed denial-of service.DDos is a type of DOS attack where multiple compromised systems are used to target a single system causing a Denial of Service (DoS) attack. In Figure-2, the architecture of DDoS attack is shown. In the diagram, it is shown that the attacker creates a network of computers and attack the victim hence consumes its all resources. The very first task of attacker is to identify the vulnerable host then intruder install the new program called attack tools to the host. That entire host that executes these tool programs is called Zombies and these Zombies can conduct any type of attack on victim as per the demand of attacker. When the operating system notices the high workload on the flooded

service, it will start to provide more computational power to cope with the additional workload. The attacker can flood a single system based address in order to perform a full loss of availability on the intended service.

There is various type of Dos attacks like-

Figure-2: Architecture of DDoS

2.1.1)X-DoS (Extensible Markup Language (XML) based Denial of Service) attacks

It is Parsing attack. When a XML message is sent with a Digital signature and sent to victim then victim's parser parse all signature hence consumes all CPU cycles.

2.1.2.H-DoS (Hypertext Transfer Protocol (HTTP) based Denial of Service) attack

HTTP Flooder launches this attack. HTTP Flooder starts almost 1500 threads that consume the entire communication channel of victim.

2.2. Side-channel Attacks

These techniques allow an attacker to monitor the analog characteristics of power supply and interface connections, thus they can be used to access the chip surface directly, so the attacker can observe, manipulate, and interfere with the device or it can be useful to extract confidential information from the VMs.After identifying where a particular target VM is likely to reside, an attacker can then instantiate new VMs until one is placed co-resident with the target VM. After the successful placement of malicious VM to targeted VM then extract the confidential information from the targeted VM called as a Side channel attack . Side channel attack requires two main steps:

Placement

First attacker has to identify the location where the target VM resides. The location can be identified with various network-probing tools. After identifying the exact location of target VM the Malicious VM put near to the target VM in such a way that both the VMs share the same physical servers and resources such as cache, pipelines, network access etc.

Extraction

After successfully placement of the malicious VM to the targeted VM, the confidential information, files and documents present in target VM can be easily extracted.

2.3. Authentication attacks

Authentication attack is a type of data stealing attack. It is the most traditional attack in which the attacker tends to breach the user account. Here, security can be provided at IaaS like information protection and data encryption. In data security, there are various services to implement the authentication like encipherment , digital signature and authentication exchange. In all cloud infrastructure a username and password is used for authentication. Hence, authentication is a weak point in any infrastructure that can be targeted easily. The strength of authentication mechanism depends on number of things it depends that can be grouped as:

- **Group1:** Things a user knows like username, email address, PIN and password and their complexity and strength.
- **Group-2:** Things a user possess like inbox, credit card, mobile phone, security token.
- **Group-3:** Things only a user has that are based on some biometrics like fingerprints, voice recognition, retina recognition, face recognition.

2.4. Cloud Malware Injection Attack

Malware injection attack is spreading like wildfire these days, and countless websites have been affected. The attack is done via a compromised FTP, and many believe that the virus can actually "sniff out" FTP passwords and send it back to the hacker. The hacker then uses your FTP password to access your website and add malicious iframe coding to infect other visitors who browse your website. In this attacker may injecting malicious service,code or virtual machine into the Cloud system. Such kind of Cloud malware could serve any particular purpose the adversary is interested in, ranging from eavesdropping via subtle data modifications to deadlock or blockings. In cloud a failure can mainly caused by either failure in hardware that is defect in IaaS or due to defect in Saas hence the attacker injects the malicious service in either Iaas or SaaS of the cloud servers. This type of attack is also known as a meta-data spoofing attack. The main idea of the Cloud Malware Injection attack is that an attacker uploads a manipulated copy of a victim's service instance so that some service requests to the victim service are processed within that malicious instance. In order to achieve this, the attacker has to gain control over the victim's data in the cloud system (e.g. using one of the attacks described above). In terms of classification, this attack is the major representative of exploiting the service-to-cloud attack surface . The attacker controlling the cloud—exploits its privileged access capabilities to the service instances in order to attack that service instance's security domains.

2.5. Man-In-The-Middle Cryptographic Attacks

This attack is carried out when an attacker places himself between two users. Attacker being in the middle of the two communicating parties' can intercept the communication.

2.6. Unknown sophisticated attacks

Hackers are so patiently working out for finding out the vulnerabilities on the cloud systems since breaking a cloud system will provide major advantages. The method that they are using is still ambiguous. Hackers are always a step ahead of the security specialists. The method to which the attack is being done is always sophisticated which means

no one except the attacker does not know about the finding out of loopholes.

2.7. Accountability Check Problem

When a user requests a service from cloud after authenticating the user, service provider launches a VM instance for that user that can provide the service to the user. For that instance the number of data transfer, number of CPU cycles, Time duration for which that instance is reserved by user all these information is recorded. As the payment method in a cloud System is "No use No bill".. So, when an attacker has launch some a malicious service which consumes a lot of computational power and storage from the cloud server, then all these charges are deducted from the account of the legitimate user. However, the customer is not aware of the attack and until the main cause of the CPU, usage is detected, the providers will charge the customers first. As a result, a dispute arises and business reputations are hampered. All the focus for charging is based on the recorded parameters. In most cases, the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the customer must ensure that the provider has taken the proper security measures to protect their information.

The cloud security issues can be classified into two categories:-

- Issues faced by cloud providers (organizations providing software, platform, or infrastructure-as-a-service via the cloud)
- issues faced by their customers

3. VARIOUS SECURITY CONCERNS:

Table 1 illustrates the various security concerns of cloud. The table depicts all the relevant field of security related aspect and their meaning with respect to cloud.

Table1: Various Security Concerns Of Cloud

S.No.	Issues	Meaning
1.	Governance and Enterprise Risk Management	The ability of an organization to govern and measure enterprise risk introduced by cloud computing. Items such as legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and how international boundaries may affect these issues.
2.	Information Management and Data Security	The prime concern is security and Managing data that is placed in the cloud It include who manages encryption and decryption of data? , Where is your data more secure, on your local hard driver or on high security servers in the cloud? Who is responsible for data confidentiality, integrity, and availability are mentioned?
3.	What are the service level agreement (SLA) terms?	The SLA serves as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided.
4.	Compatibility of storage services of various Clouds.	Storage services provided by one cloud vendor may be incompatible with another vendor's services if user decides to move from one to the other (e.g. Microsoft cloud is incompatible with Google cloud).
5.	What is the Traditional Security, disaster recovery/business continuity plan (DR/BCP)?	While you may not know the physical location of your services, it is physically located somewhere. All physical locations face threats such as fire, storms, natural disasters, and loss of power. In case of any of these events, how will the cloud provider respond, and what guarantee of continued services are they promising?
6.	Security of Hypervisors'?	A hypervisor, also called a virtual machine manager, is a program that allows multiple operating systems to share a single hardware host. Each operating system appears to have the host's processor, memory, and other resources all to itself. It includes risk associated with multi-tenancy, VM isolation, VM co-residence, hypervisor vulnerabilities, etc. It is concerned with security issues surrounding system/hardware virtualization, rather than a more general survey of all forms of virtualization.
7.	What happens if there is a security breach?	If a security incident occurs, what support will you receive from the cloud provider? While many providers promote their services as being unhackable, cloud based services are an attractive target to hackers.
8.	Portability and Interoperability	The ability to move data/services from one provider to another, or bring it entirely back in-house. Together with issues surrounding interoperability between providers.
9.	What is the long-term viability of the provider?	How long has the cloud provider been in business In addition, what is their record of accomplishment? If they go out of business, what happens to your data? Will your data be returned, and if so, in what format?
10.	Do you have the right to audit?	In addition to producing logs and audit trails, cloud providers work with their customers to ensure that these logs and audit trails are properly secured maintained for as long as the customer requires, and are accessible for the purposes of forensic investigation.
11.	What are your regulatory requirements?	Organizations operating in the US, Canada, or the European Union have many regulatory requirements that they must abide by (e.g., ISO 27002, Safe Harbor, ITIL, and COBIT). You

		must ensure that your cloud provider is able to meet these requirements and is willing to undergo certification, accreditation, and review.
13.	Application Security	Securing application software that is running on or being developed in the cloud. This includes items such as whether it is appropriate to migrate or it is more efficient to design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS). However, the threats to the applications are going to be exposed to in a cloud environment will be more than those experienced in a traditional data center. This creates the need for rigorous practices that must be followed when developing or migrating applications to the cloud.

Prior to cloud the entire tech world is based on traditional computing but evolution of cloud computing revolutionized the tech world .It has many benefits but use of virtualization reveals many security concerns. Cloud is multi-tenant, scalable network ; use of hypervisors, virtual switches causes many attacking point. Comparative study between cloud computing and traditional computing on certain security concerns mentioned below:

Table 2: Comparative study between cloud computing and traditional computing

S.no.	Security Feature	Traditional computing	Cloud computing
1.	Infrastructure	Traditional computing system consist of routers, hubs, switches, access policies etc. all these things are built in house and all aspects of security are left to local administrator.	In cloud, computing the Infrastructure is built and managed by third party, i.e. company runs its stuff at some services that are not owned and maintained by it.
2.	Access Control	Here, accesses control is managed by companies own policies and managed locally.	As cloud third party maintains resources so it is up to that third party whether they consider the guidelines given by company.
3.	Encryption	Encryption is provided by IPSec (internet protocol security).In traditional computing encryption is cheaper than cloud.	Encryption is best for securing cloud data in transit. Encryption can be done by encryption algorithm but it might cause delay and difficulty in access. For this data fragmentation and data, concealment is used. Trend micro work is being done about an encryption scheme for public cloud to apply encryption in every instance of VM instance, homomorphic (encryption provides manipulation on encrypted data without knowing the decryption key).
4.	Physical Security	All resources and infrastructure are managed locally hence, accesses of resources are given to the required person.	In cloud all resources are managed and controlled by third party i.e. CSP (Cloud Service Provider).Here, the access given to the authorized person but that authorized person are invisible to the client.
5.	Data Recovery	Data Recovery is expensive in traditional computing because organization needs to maintain many servers in order to ensure that all data are backed up. In Traditional computing the entire data of company is placed at one place so any natural disaster can destroy it completely.	All data are at remote location so it is easy to maintain a record in case of any natural disaster because it is possible that data is available at some other location. Data recovery in cloud is very efficient in cloud and it decreases the downtime.
6.	Security	Security in traditional computing is provided by firewalls, internet protocols, policies and various other protocols like HTTP(Hypertext transfer protocol),SSL(Secure Socket Layer: developed by Netscape),SMTP(Simple Mail Transfer Protocol),TCP/IP,TLS etc but here, all maintenance are done locally and controlled by local admin.	In cloud computing various aspects like Data center security, Server security, Client security, Password security, Access control etc; should to be maintained. But here, security is maintained by third party and assured to client by SLA(Service Level Agreement) that dictates the counter measures that would be taken if any type of security breach occurs or any type of data get loosed.
7.	Virtualization	In traditional computing a lot of hardware component are required because all functions are done and managed by only one servers or many other servers are deployed that increases the cost overhead.	It is developed to minimize the cost overhead of the system. In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. A Hypervisor between the hardware and the OS enables multiple virtual machines run on the top of a single physical machine. Not only can data

			center security teams replicate typical security controls for the data center at large to secure the virtual machines but here security aspects arises like a single host having many virtual machines that can be attacked by any guest operating system.

4. Conclusion

This paper reflects the cloud attacks i.e. what are the various attacks that still threatening the cloud service provider, client and customer to put their data in cloud. The paper also enlightens some of the security concerned that must be considered before adopting cloud .In the mentioned security concerns some very relevant and critical. Various researchers are working on those aspects and trying to mitigate their impact. The most considerable area is Security that can be breached in many forms. The various security concerns like security of data centers, various encryption techniques that can be applied without decreasing the seep and performance, Hypervisor security. In this paper, a comparison is shown between traditional computing and cloud computing that reflects pros and cons of both techniques.

References

[1] Security and Privacy in Cloud Computing, Zhifeng Xiao and Yang Xiao, Senior Member, IEEE

[2] An Overview and Study of Security Issues & Challenges in Cloud Computing, International Journal of Advanced Research in Computer Science and Software Engineering

[3] Security guidance for critical areas of focus in cloud computing v3.0, csaguide.v3.0, http://cloudsecurityalliance.org/

[4] Cloud computing security - Wikipedia, the free encyclopedia.htm

[5] Introduction to Cloud Computing and Virtualization by Mayank Mishra, Sujesha Sudevalayam, PhD Students CSE, IIT Bombay

[6] Cloud Computing Virtual Cloud Security Concerns TechNet Magazineimp.htm

[7] Cloud Computing vs. Traditional Internet Setting: Which One is More Secure By Mansooreh Moghadam,wendy Sterkel, Cameron University Spring 2012, IT-4444.

[8] Survey on Security Issues and Problems in Cloud Computing Virtual Machines (IJCSIT) International Journal of Computer science and Information Technologies, Vol. 4 (6) , 2013, 755-760.

[9]Authentication Attacks and Counter-measures ICT.govt.nz.htm.

[10] Overview of Attacks on Cloud Computing Ajey Singh, Dr. Maneesh Shrivastava, International Journal of Engineering and innovative Technology (IJEIT) , Volume 1, Issue 4, April 2012 .

[11]Security Attacks and Solutions in Clouds ,Kazi Zunnurhain and Susan V. Vrbsky Department of Computer Science The University of Alabama Tuscaloosa, AL 3548-0290