ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 06, pp.33263-33268, June, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

SURVEY ON THREATS AND ATTACKS IN CLOUD INFRASTRUCTURE

***Diksha Nagpal and Dr. Deepti Sharma**

Department of Computer Science and Engineering, Advanced Institute of Technology & Management, Palwal

ARTICLE INFO

Article History:
Received 17th March, 2016
Received in revised form
17th April, 2016
Accepted 21st May, 2016
Published online 30th June, 2016

Key words:

DDOS, Ping of Death,
Land Attack, Vulnerabilities.

ABSTRACT

Cloud computing has brought revolution in IT industry. There are major benefits of using cloud environment due to the better utilization of resources and reduced cost. Cloud infrastructure consists of the use of virtual machines like hypervisor etc. and it is similar to the large network. The cloud storage consists of huge amount of information and that can be shared from anywhere in the world with secure access. Wherever, the network is designed and internet is being used that becomes vulnerable to attacks. And as the technology is advancing, the cyber criminals have also become smarter and can identify the vulnerabilities, threats and can perform attacks on the cloud system. So,this paper aims at describing the different types of threats and attacks in the cloud infrastructure.

Citation: Diksha Nagpal and Dr. Deepti Sharma, 2016. "Survey on threats and attacks in cloud infrastructure", *International Journal of Current Research*, 8, (06), 33263-33268.

INTRODUCTION

Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. Cloud computing is a model for enabling convenient, on-demand 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. Some other benefits to users include scalability, reliability, and efficiency. Scalability means that cloud computing offers unlimited processing and storage capacity. The cloud is reliable in that it enables access to applications and documents anywhere in the world via the Internet. Cloud computing is often considered efficient because it allows organizations to free up resources to focus on innovation and product development.Alongwith the advantages there are security issues also due to the sharing of resources and network. In this paper, the various threats, vulnerabilities and attacks are being described.

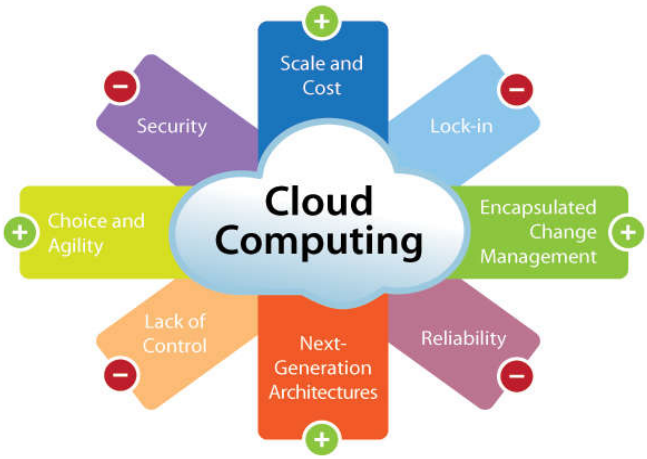

Figure 1. Cloud Computing

Cloud computing has become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as

Corresponding author: Diksha Nagpal,
Department of Computer Science and Engineering, Advanced Institute of Technology & Management, Palwal

well as availability. Some cloud vendors are experiencing growth rates of 50% per year, but being still in a stage of infancy, it has pitfalls that need to be addressed to make cloud computing services more reliable and user friendly. Internet security is highly interdependent the launch of DDoS attack depends upon the global internet security. Limited Internet resources Each Internet host has limited resources that can be consumed by a sufficient number of users. Control is distributed Due to privacy concerns of the Internet, sometimes it is nearly impossible to investigate the cross network behavior and to deploy certain global security mechanism. Multipathrouting this causes authentication process difficult and hence it may leads to unauthorized activities. Intermediate router forwards IP packet from source to destination without knowledge about the IP packet whether it is genuine or not.

I.Threatsincloud computing

The following are the top security threats in a cloud environment:

Ease of Use

The cloud services can easily be used by malicious attackers, since a registration process is very simple, because we only have to have a valid credit card. In some cases we can even pay for the cloud service by using PayPal, Western Union, Payza, Bitcoin, or Litecoin, in which cases we can stay totally anonymous. The cloud can be used maliciously for various purposes like spamming, malware distribution, botnet C&C servers, DDoS, password and hash cracking.

Secure Data Transmission: When transferring the data from clients to the cloud, the data needs to be transferred by using an encrypted secure communication channel like SSL/TLS. This prevents different attacks like MITM attacks, where the data could be stolen by an attacker intercepting our communication.

Insecure APIs: Various cloud services on the Internet are exposed by application programming interfaces. Since the APIs are accessible from anywhere on the Internet, malicious attackers can use them to compromise the confidentiality and integrity of the enterprise customers. An attacker gaining a token used by a customer to access the service through service API can use the same token to manipulate the customer's data. Therefore it's imperative that cloud services provide a secure API, rendering such attacks worthless.

The security and availability of cloud services from authentication and access control to encryption and activity monitoring depend on the security of the API. Risk increases with third parties that rely on APIs and build on these interfaces, as organizations may need to expose more services and credentials. Weak interfaces and APIs expose organizations to security issues related to confidentiality, integrity, availability, and accountability. APIs and interfaces tend to be the most exposed part of a system because they're usually accessible from the open Internet. The Security Alliance recommends adequate controls as the "first line of defense and detection." Threat modeling applications and systems, including data flows and architecture/design, become important parts of the development lifecycle. The CSA also recommends security-focused code reviews and rigorous penetration testing

Malicious Insiders: Employees working at cloud service provider could have complete access to the company resources. Therefore cloud service providers must have proper security measures in place to track employee actions like viewing a customer's data. Since cloud service provides often don't follow the best security guidelines and don't implement a security policy, employees can gather confidential information from arbitrary customers without being detected. The insider threat has many faces: a current or former employee, a system administrator, a contractor, or a business partner. The malicious agenda ranges from data theft to revenge. In a cloud scenario, a hellbent insider can destroy whole infrastructures or manipulate data. Systems that depend solely on the cloud service provider for security, such as encryption, are at greatest risk.

Shared Technology Issues: The cloud service SaaS/PasS/IaaS providers use scalable infrastructure to support multiple tenants which share the underlying infrastructure. Directly on the hardware layer, there are hypervisors running multiple virtual machines, themselves running multiple applications. On the highest layer, there are various attacks on the SaaS where an attacker is able to get access to the data of another application running in the same virtual machine. The same is true for the lowest layers, where hypervisors can be exploited from virtual machines to gain access to all VMs on the same server (example of such an attack is Red/Blue Pill). All layers of shared technology can be attacked to gain unauthorized access to data, like: CPU, RAM, hypervisors, applications, etc.

Data Loss: The data stored in the cloud could be lost due to the hard drive failure. A CSP could accidentally delete the data, an attacker might modify the data, etc. Therefore, the best way to protect against data loss is by having a proper data backup, which solves the data loss problems. Data loss can have catastrophic consequences to the business, which may result in a business bankruptcy, which is why keeping the data backed-up is always the best option.

Data Breach: When a virtual machine is able to access the data from another virtual machine on the same physical host, a data breach occurs – the problem is much more prevalent when the tenants of the two virtual machines are different customers. The side-channel attacks are valid attack vectors and need to be addressed in everyday situations. A side-channel attack occurs when a virtual machine can use a shared component like processor's cache to access the data of another virtual machine running on the same physical host.

Account/Service Hijacking: It's often the case that only a password is required to access our account in the cloud and manipulate the data, which is why the usage of two-factor authentication is preferred. Nevertheless, an attacker gaining access to our account can manipulate and change the data and therefore make the data untrustworthy. An attacker having access to the cloud virtual machine hosting our business

website can include a malicious code into the web page to attack users visiting our web page – this is known as the watering hole attack. An attacker can also disrupt the service by turning off the web server serving our website, rendering it inaccessible.

Unknown Risk Profile: We have to take all security implications into account when moving to the cloud, including constant software security updates, monitoring networks with IDS/IPS systems, log monitoring, integrating SIEM into the network, etc. There might be multiple attacks that haven't even been discovered yet, but they might prove to be highly threatening in the years to come.

Denial of Service: An attacker can issue a denial of service attack against the cloud service to render it inaccessible, therefore disrupting the service. There are a number of ways an attacker can disrupt the service in a virtualized cloud environment: by using all its CPU, RAM, disk space or network bandwidth.DoS attacks consume large amounts of processing power, a bill the customer may ultimately have to pay. While high-volume DDoS attacks are very common, organizations should be aware of asymmetric, application-level DoS attacks, which target Web server and database vulnerabilities. Cloud providers tend to be better poised to handle DoS attacks than their customers. The key is to have a plan to mitigate the attack before it occurs, so administrators have access to those resources when they need them.

Lack of Understanding: Enterprises are adopting the cloud services in every day operations, but it's often the case they don't really understand what they are getting into. When moving to the cloud there are different aspects we need to address, like understanding how the CSP operates, how the application is working, how to debug the application when something goes wrong, whether the data backups are already in place in case the hard drive dies, etc. If the CSP doesn't provide additional backup of the data, but the customer expects it, who will be responsible when the hard drive fails? The customer will blame the CSP, but in reality it's the customer's fault, since they didn't familiarize themselves enough with the cloud service operations – the result of which will be lost data.

User Awareness: The users of the cloud services should be educated regarding different attacks, because the weakest link is often the user itself. There are multiple social engineering attack vectors that an attacker might use to lure the victim into visiting a malicious web site, after which he can get access to the user's computer. From there, he can observe user actions and view the same data the user is viewing, not to mention that he can steal user's credentials to authenticate to the cloud service itself. Security Awareness is an often overlooked security concern.

Cloud service abuses: Cloud services can be commandeered to support nefarious activities, such as using cloud computing resources to break an encryption key in order to launch an attack. Other examples including launching DDoS attacks, sending spam and phishing emails, and hosting malicious content.

Providers need to recognize types of abuse -- such as scrutinizing traffic to recognize DDoS attacks -- and offer tools for customers to monitor the health of their cloud environments.

Customers should make sure providers offer a mechanism for reporting abuse. Although customers may not be direct prey for malicious actions, cloud service abuse can still result in service availability issues and data loss.

II.Vulnerabilities in cloud computing

When contemplating to migrate to cloud computing, you have to consider the following security issues for you to enhance your data safety.

Session Riding

Session riding occurs when an online attacker steals an internet user's cookie to use the application later as the real user. The attackers might also use the CSRF attacks for them to trick the user to send authentic requests to random websites to accomplish various missions.

Virtual Machine Escape

Within virtualized settings, the physical servers operate multiple virtual apparatuses on top of the hypervisors. An online attacker can remotely exploit a hypervisor by using a weakness present in that particular hypervisor. However, such vulnerabilities are pretty rare, but they are real. Also, a virtual machine can avoid the virtualized sandbox setting to gain access to the hypervisor. Consequently, all the virtual machines ultimately run on the virtual machine.

Unsafe Cryptography

Cryptography algorithms normally use random number generators. They use unpredictable information sources to produce actual random numbers that are needed to get a large entropy pool. When the random number generators provide only a limited entropy pool, the numbers can be forced. In a client's computer, the major source of randomization is user mouse operations and the key presses. Servers however normally operate without user interaction. That consequently means that there will be a lower number of sources for randomization. Hence, the virtual machines usually rely on the sources that are available to them. That could lead to easily guessable numbers that do not give much uncertainty in cryptographic algorithms.

CSP Lock-in

You have to choose a provider that has guarantee cloud security will enable you to shift easily to another provider when necessary. You do not want to choose a CSP that will force you to use its services. That is because sometimes you would prefer to use a CSP in one thing and another CSP for something different.

These are the following vulnerabilities in cloud computing-

ID	Vulnerabilities	Description
V01	Insecure interfaces and APIs	Cloud providers offer services that can be accessed through APIs (SOAP, REST, or HTTP with XML/JSON). The security of the cloud depends upon the security of these interfaces. Some problems are: a) Weak credentials b) Insufficient authorization checks c) Insufficient input-data validation Also, cloud APIs are still immature which means that are frequently updated. A fixed bug can introduce another security hole in the application.
V02	Unlimited allocation of resources	Inaccurate modeling of resource usage can lead to overbooking or over-provisioning.
V03	Data-related vulnerabilities	a) Data can be colocated with the data of unknown owners (competitors, or intruders) with a weak separation. b) Data may be located in different jurisdictions which have different laws. c) Incomplete data deletion – data cannot be completely removed. d) Data backup done by untrusted third-party providers. e) Information about the location of the data usually is unavailable or not disclosed to users. f) Data is often stored, processed, and transferred in clear plain text
V04	Vulnerabilities in Virtual Machines	a) Possible covert channels in the colocation of VMs. b) Unrestricted allocation and deallocation of resources with VMs. c) Uncontrolled Migration - VMs can be migrated from one server to another server due to fault tolerance, load balance, or hardware maintenance. d) Uncontrolled snapshots – VMs can be copied in order to provide flexibility, which may lead to data leakage e) Uncontrolled rollback could lead to reset vulnerabilities - VMs can be backed up to a previous state for restoration, but patches applied after the previous state disappear f) VMs have IP addresses that are visible to anyone within the cloud - attackers can map where the target VM is located within the cloud (Cloud cartography)
V05	Vulnerabilities in Virtual Machine Images	a) Uncontrolled placement of VM images in public repositories. b) VM images are not able to be patched since they are dormant artifacts.
V06	Vulnerabilities in Hypervisors	a) Complex hypervisor code. b) Flexible configuration of VMs or hypervisors to meet organization needs can be exploited
V07	Vulnerabilities in Virtual Networks	Sharing of virtual bridges by several virtual machines.

III.Attacks and intrusions in cloud computing

A.Attacks on hypervisor or virtual machines

An attacker may successfully control the virtual machines by compromising the hypervisor. The most common attacks on virtual layer are SubVir, BLUEPILL, and DKSM which enable hackers to supervise host through hypervisor. Attackers target the hypervisor or VMs to access them by exploiting the zero-day vulnerabilities in virtual machines , prior to the developers awareness about such exploits.

B.User to root (U2R) attacks

The attacker uses password sniffing to access a genuine user's account which enables him to obtain root privileges to a system by exploiting vulnerabilities, e.g. Root shells can be created by using Buffer overflows from a root-level process.

C.Backdoor channel attacks

Hackers can remotely access the infected machines by exploiting this passive attack to compromise the confidentiality of user information. Hacker can use backdoor channels to get control of victim's resources and utilize it as zombie to launch DDoS attack.

D.Denial of Service (DoS) attack

The attacker exploits zombies for sending a large number of network packets to overwhelm the available resources. Consequently, legitimate users are unable to access the services offered over the Internet. In cloud environment, the attacker may send huge number of requests through zombies to access VMs thus disabling their availability to legitimate users which is called DoSattack.As large magnitudes of data are moving onto the cloud, the attackers are keener to exploit the vulnerabilities associated with cloud and thereby to steal the sensitive data. Among the various threats to cloud computing, Denial of Service(DoS) attacks can prove to be the deadliest attack and even the Cloud Security Alliance has identified DoS attack as one of the nine major threats. In DoS attack, the intruder overloads the target system with service requests so that it cannot respond to any further requests and hence resources will be made unavailable to its users. Distributed Denial of Service (DDoS) attack makes use of several compromised machines called zombies to launch DoS attack on the target machine and the service is disrupted or delayed. DDoS attacks are getting more frequent these days and hence proper intrusion detection systems has to be deployed.

Types of DoS Attacks

The DDoS attacks can beclassified into three categories.

Volume Based Attacks/Bandwidth Based Attacks

This attack makes an attempt to overload the victim with large amounts of junk data thereby consuming the network bandwidth and resources. Examples include UDP floods, ICMP floods.

Protocol Attacks

The attack tries to take advantage of the lacuna associated with various network protocols to overload the target's resources. Examples include Ping of Death, Smurf attack, SYN floods, fragmented packet attack etc.

Application Layer Attacks

The attack concentrates on specific web applications and sends HTTP requests beyond the limits it can handle. This kind of attack includes HTTP DDoS attack and XML DDoS attacks or REST based attacks.

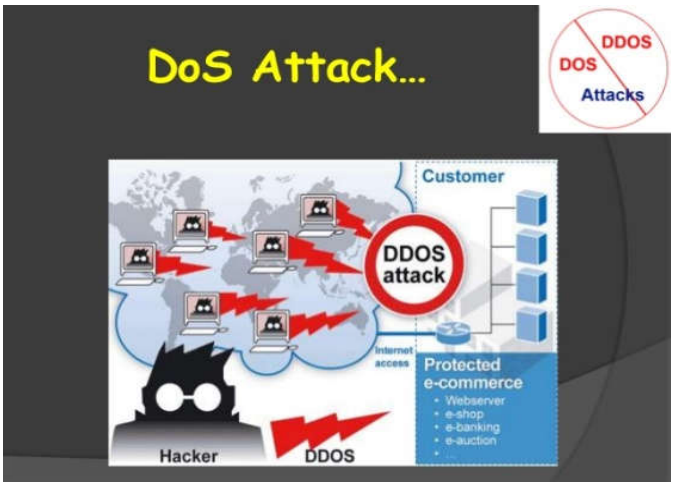

Figure 2. DDOS Attack

A DDoS includes different types of attacks

i)IP spoofing attack

In the Internet Protocol (lP) spoofing attack, packet transmissions between the end user and the cloud server can be intercepted and their headers modified such that the IP source field in the IP packet is forged by either a legitimate IP address, or by an unreachable IP address.

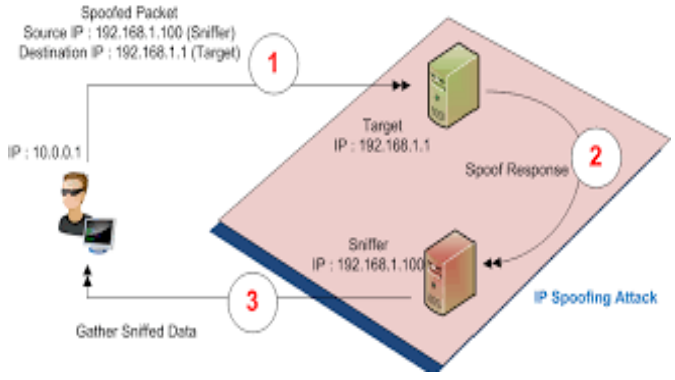

Figure 3. IP Spoofing

ii)SYN flooding attack

A typical three-way handshake between a legitimate user and the server begins by sending a connection request from the legitimate user to the server in the form of a synchronization (SYN) message. Then, the server acknowledges the SYN by sending back (SYN-ACK) a request to the legitimate user. Finally, the legitimate user sends an ACK request to the server to establish the connection. SYN flooding occurs when the attacker sends a huge number of packets to the server but does not complete the process of the three-way handshake. As a result, the server waits to complete the process for all of those packets, which makes the server unable to process legitimate requests.

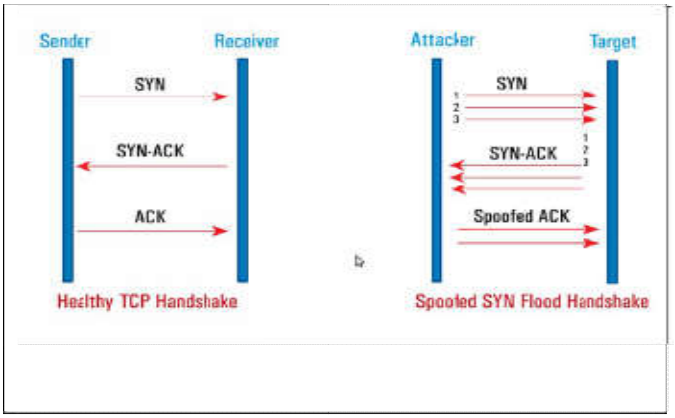

Figure 4. Syn Flooding

iii)Smurf attack

In a smurf attack, the attacker sends a large number of Internet Control Message Protocol (lCMP) echo requests. These requests are spoofed such that its source IP address is the victim's IP, and the IP destination address is the broadcast IP address.As a result, the victim will be flooded with broadcasted addresses. The worst case occurs when the number of hosts who reply to the ICMP echo requests is too large.

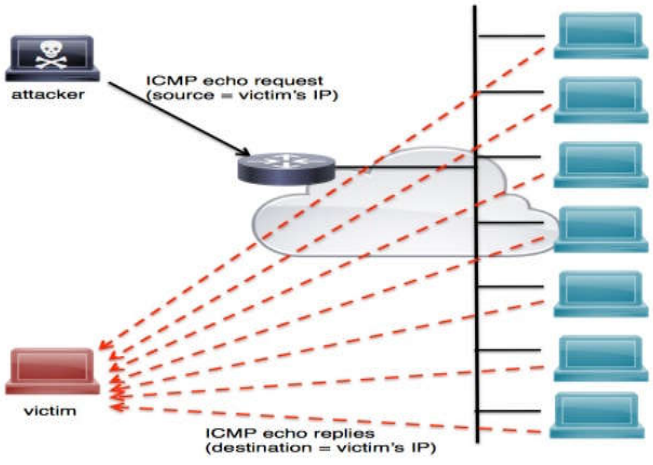

Figure 5. Smurf Attack

iv)Buffer overflow attack

In a buffer overflow attack, the attacker sends an executable code to the victim in order to take advantage of buffer

overflow vulnerability. As a result, the victim's machine will be controlled by the attacker. The attacker could either harm the victim's machine or use the infected machine to perform an internal cloud-based DDoS attack.

v)Ping of death attack

In the ping of death attack, the attacker sends an IP packet with a size larger than the limit of the IP protocol, which is 65,535 bytes. Handling an oversized packet affects the victim's machine within the cloud system as well as the resources of the cloud system.

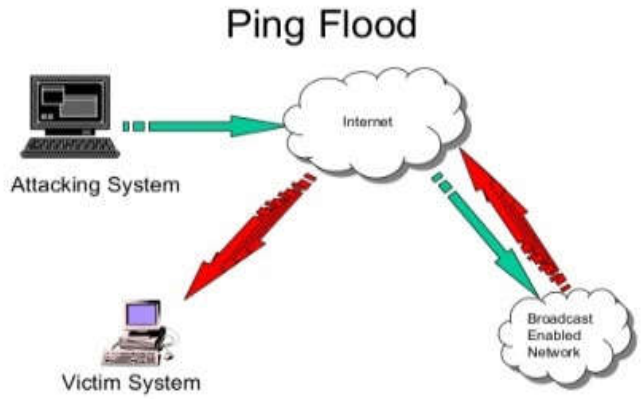

Figure 6. Ping of death attack

vi)Land attack

This attack uses the "Land.c" program to send forged TCP SYN packets with the victim's IP address in the source and destination fIelds. In this case, the machine will receive the request from itself and crash the system. Such an attack is prevented in recent networking devices and operating systems by dropping ICMP packets that contain the same IP address in the source and destination fIelds.

vii)Teardrop attack

This kind of attack uses the "Teardrop.c" program to send invalid overlapping values of IP fragments in the header of TCP packets. As a result, the victim's machine within the cloud system will crash in the re-assembly process.

E.Cloud Malware Injection Attack

A first considerable attack attempt aims at injecting a malicious service implementation 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 full functionality changes or blockings. This attack requires the adversary to create its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and add it to the Cloud system. Then, the adversary has to trick the Cloud system so that it treats the new service implementation instance as one of the valid instances for the particular service attacked by the adversary. If this succeeds, the Cloud system automatically redirects valid user requests to the malicious service implementation, and the adversary's code is executed. A promising countermeasure approach to this threat consists in the Cloud system performing a service instance integrity check prior to using a service instance for incoming requests.

Figure 7. Malware Attack

F.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. Side-channel attacks have emerged as a kind of effective security threat targeting system implementation of cryptographic algorithms.

Conclusion

Due to the sharing of resources and access through internet, there are many types of threats and vulnerabilities of virtual machines that are listed above. These threats and vulnerabilities leads to the various types of attacks popularly like DDOS and in that also various kinds of DDOS attacks. Not only DDOS attacks which are performed by intruding the malware inside the cloud environment and also by entering into system by using administratoraccount. These attacks can cause serious damages to the cloud system and all the users will not be able to access the information affecting business activities. Alongwith, these devices like Unified Threat Management (UTM) can also be implemented as the future work for the security of the Cloud system.So, all the threats, risks and vulnerabilities can be avoided and attacks can also be prevented.

REFERENCES

Ajey Singh, Dr. ManeeshShrivastava, 2012. "Overview of Attacks on Cloud Computing", *International Journal of Engineering and Innovative Technology (IJEIT)*, Volume 1, Issue 4.

https://www.priv.gc.ca/resource/fs-fi/02_05_d_51_cc_e.pdf

Marwan Darwish, AbdelkaderOuda, Luiz Fernando Capretz, "Cloud-based DDoS Attacks and Defenses", Department of Electrical and Computer Engineering University of Western Ontario London, Canada {mdarwis3,aouda,lcapretz} @uwo.ca

Raja Mohammed Jabir, SalaamIsmail RasheedKhanji, LizaAbdadallahAhmad, OmarAlfandi, Huwaida Said," Analysis of Cloud computing Attacks and Countermeasures, Jan. 31 ~ Feb. 3, 2016 ICACT2016.

SenthilKumar, M. 2013."A Secured Cloud Storage Technique To Improve Security In Cloud Infrastructure" International Conference on Recent Trends in Information Technology (ICRTIT).

Yasirmehmood, UmmeHabiba, 2013. "Intrusion Detection System in Cloud Computing: Challenges and Opportunities" 2nd National Conference on Information Assurance (NCIA).

****