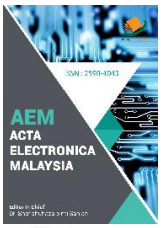
ZIBELINE INTERNATIONAL PUBLISHING

ISSN: 2590-4043 (Online)
CODEN: AEMCDV

Acta Electronica Malaysia (AEM)

DOI: http://doi.org/10.26480/aem.02.2025.61.65



CrossMark

REVIEW ARTICLE

TYPES OF ATTACKS OVER CLOUD COMPUTING WITH PREVENTION TECHNIQUES

Zhou Lin[a*], Usman Akhtar[b]

[a] School of Physics and Electronic Information Engineering, Yuncheng University, Yuncheng, Shanxi, China.
[b] Faculty of Electrical & Electronics Engineering, University of South Asia, 47-J-III, Gulberg-III, Lahore, 54660, Pakistan.
**Corresponding Author Email: XiaofeiHan@protonmail.com*

ARTICLE DETAILS

Article History:

Received 20 September 2025
Revised 26 October 2025
Accepted 28 November 2025
Available online 31 December 2025

ABSTRACT

Cloud computing has a significant role in our daily life. Having many features, it made our life easier. Keeping cloud environment reliable and secure is very essential in order to support large number of users and many smart devices. Now-a-days Cloud computing security is one of the important challenging fields. The biggest security threat for services availability in Cloud Computing is Distributed Denial of Service (DDoS) attack. A major attribute to DDoS attack that hides attacker's identity is IP address spoofing. With the passing of time DDoS attack becomes powerful, the attack may be minimized if it is detected at first. So we focused on prevention mechanism against the attack for securing the cloud environment.

KEYWORDS

Cloud Computing, DDoS attack and attributes, IP address spoofing, Side Channel attack, authentication attack, Malware Injection Cloud Attack, Man in the Middle.

1. INTRODUCTION

Computing technology has blessed today's world with its features. Without Cloud computing it won't be possible for increasing number of users to enjoy high speed internet. In recent few years cloud computing has been used to provide services to the clients either using private, public or hybrid cloud models. Cloud service model contains of three types: Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) (Khorshed et al., 2012). The attacks damages both valuable time and money. The possibility to diminish the attacks of Cloud system will help the end users to enjoy a secure Cloud environment. There are many destructive Cloud attacks that destroys the Cloud environment in few seconds if there are no prevention mechanisms. Cloud Computing's security issues can be viewed with CIA which is Confidentiality, Integrity and Availability. The biggest security threat for service availability in Cloud Computing is known as DDoS attack (Tsai, et al., 2010). Networking system's machine is targeted and a large number of traffics are generated by which the server system in Cloud environment is attacked. The cloud server gets pressurized for processing large number of traffic. As the time increases the arrival of packet rate becomes high if no prevention mechanism available in Cloud system. As a result, the cloud system fails to serve its users. This avoids permitted Cloud users for accessing user's pool which is provided by Cloud Providers through consuming network bandwidth and flooding. One of the attributes of DDoS attack is IP Address Spoofing, where source IP Address is copied fraudulently. In this research paper different ways are discussed through which we can detect spoofed IP packet during a DDoS attack in Cloud Computing.

2.RELATED WORK

Starting late, various investigators suggested assorted approaches to manage inspecting security issues of cloud preparing. Meiko Jensen et al. Consider the specific security issues rising up out of the utilization of cloud organizations and the shrouded progressions used to collect these cross-space between related facilitated endeavors. This work concentrates more on web organizations related security issues and concentrates less on check factor (Subashini and Kavitha, 2011). Hassan Takabi et al., have recognized circulated processing as a steady force because of its inert limit benefits. The makers include the need to have legitimate parts to manage the security and assurance perils in cloud. The work analyzes the security challenges including customer affirmation, get the chance to control, approach joining, trust the administrators and organization the board and proposes a comprehensive security framework for dispersed figuring (Jensen et al., 2009; Takabi, et al., 2010). Hsin-Yi Tsai et al in their work researches the security issues in different assistance movement models from the perspective of Virtualization (Hsin-Yi, et al., 2011).

S.Subashini and V.Kavitha examined the security perils looked by the cloud organization movement models and suggests a security framework that gives data security by taking care of and getting to data subject to meta-data information (Sumitra and Misbahuddin, 2013). B. Sumitra and M. Misbahuddin has audited and requested the security threats suitable to cloud condition. The work is a general portrayal of attacks and doesn't delve significant into confirmation issues. (Sumitra and Misbahuddin, 2013). Investigated the security perils, for instance, SQL imbuement blemishes, cross-site scripting, untrustworthy storing, etc as applicable to cloud condition. Regardless, the consideration is on the various layers of the framework, for instance, Network level and Application level (Bhadauria and Sanyal, 2012). R.C.William et al. Discusses the insider threats in disseminated processing. The makers consider the insiders from three exchange perspectives and the possible impact of each insider on cloud Security. Nevertheless, this work concentrates just on a specific order of approval ambush on cloud (William et al., 2022).

3.SECURITY ATTACKS ON CLOUD COMPUTING

With the advancement in cloud computing, the vulnerabilities are being exploited and loop holes are raveling. Attackers now look on these potential attacks on cloud computing: -

Quick Response Code	Access this article online	
	Website: www.actaelectronicamalaysia.com	**DOI:** 10.26480/aem.02.2025.61.65

Cite the Article: Zhou Lin, Usman Akhtar (2025). Types Of Attacks Over Cloud Computing With Prevention Techniques. *Acta Electronica Malaysia (AEM)*, 9(2): 61-65.

3.1 Distributed Denial-of-Services Attack (DDOS)

Distributed Denial-of-Services also commonly known as DDOS attack is the methodology of overloading a targeted cloud server to an extent that it stops giving responses. Hence the already connected users don't get the resources from the Cloud server or gets very slow responses. Because typically a cloud server is accessed by so many users concurrently already a DDOS attacks becomes more threatening and effective. Some types of DDOS attacks are (Zunnurhain and Susan 2011):

- The attacker can spam the server with huge amount of data for the purposes of consuming the bandwidth and other resources. For example, ICMP floods, UDP floods etc. (Templeton and Levitt, 2003).
- The striker can take benefit and exploit the void space that is associated with the network protocols to flood the targeted server. For example, ping of death (POD), fragment packet attack (FPA) etc. (Zunnurhain and Susan 2011).
- Attackers trying to attack the server via DDOS can send unnecessary HTTP requests to the targeted cloud server until the server is not able to handle the requests anymore. For example, HTTP DDOS attack, XML etc. (Cheng, et al., 2003).

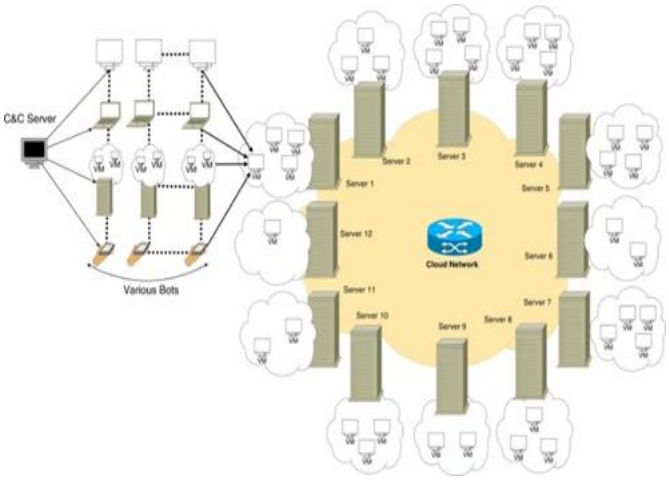


Figure 1: DDOS ATTACK

3.1.1 How DDOS Attacks can be Tackled

We can minimize DDOS attack to some extent by verifying the traffic before connecting it to the server. The approved users get permit to the server while the unapproved users wouldn't get the connection. Via this authentication mechanism server would be protected from threatening users. To make this possible firewall are used with the help of allow and deny policies (Cheng, et al., 2003). Switches now have the ability for rate minimizing concluded on ACP or access control list. This list can be programmed to minimize the rate, shape traffic, sifting false IP and can review bundles. Switches now can be set physically to set guidelines and rules (Templeton and Levitt, 2003). An application can be used to control the flow of traffic to apply some control. This can be done by making the application interact with the router and switches and analyze the packets when they make an entry in the network to check their validity and priority (Zunnurhain and Susan 2011). Another way to lessen the effects of DDOS attacks is to redirect all the traffic to a channel where it gets dump and doesn't get processed.

3.2 Malware Injection Cloud Attack

Malware Injection Attack is done to change the direction of valid user requests to the attacker implemented model and the attacker's code starts to execute. This attack can be done by injecting malware or attacker's VM in to the cloud and it pretends to be a valid user and part of the cloud. Attacker creates a malware service implementation module and somehow try to insert it in the targeted cloud. After successfully passing through the firewalls and acting as one of the valid user attacker now has to bring in some new service implementation among the valid instances this could be a virtual machine(IaaS), SaaS or PaaS. Mostly the purpose of this type of attack is to modify data, functional changes, reverse functions or block traffic. To fulfill the objective attacker has to get control over the prey data residing in the cloud. The main objective to achieve in this attack is pretending to be a service a user might request to and then transferring its request on the malicious model rather than the legit one. The taxonomy shows this type of attack exploits service to cloud attack surface.

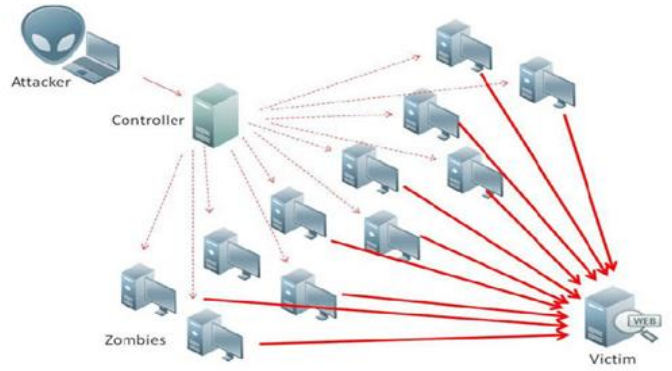


Figure 2: Malware Injection Attack

3.2.1 Countermeasure of Malware Injection Attacks

Malware injection attacks can be prevented using two approaches. A hypervisor can be implemented on the provider's side. Hypervisor is contemplated as most sophisticated and secure part of the cloud and its security is almost impossible to crack in anyway. Because information flow is so fast and integrity is said to be maintained by the given cloud server application to the customers. To keep the things flowing as they are and to prevent from ant attack we can use the hardware for security purposes or we can combine the integrity with hardware because intruding in the IaaS level of Cloud computing is comparatively difficult than any other structure. To make things stable we can use a file allocation table (FAT) to determine the integrity and validity of new objects by comparing them to the previous objects. Hypervisor manages the scheduling so it can also be used to check the FAT to integrate and validate objects of the users (Perez-Botero et al., 2013). Second approach is that we can save the state of the last instances used by the customer and can maintain the information that the user used while accessing the cloud firstly, this information can later be bused to check the new objects of the customer.

3.3 Side Channel Attacks

It aims to target the execution of cryptographic algorithms. Attacker tries to get hold of the security vulnerabilities by depositing a malicious virtual machine very near to the targeted cloud system server and then begin a side channel attack. It has become important to analyze the cryptographic techniques used to make it security stronger. Two steps used by side channel attacks [14]: VM CO Residence and placement. In this procedure attacker places the malicious device instance on the same physical address where the target is located. The other step is VM extraction. It is the process where the capability of malicious VM is used to get to the side channels and get information about the co-resident attributes. This process is very easy to execute so security must be provided to tackle this (Varadharajan, and Tupakula, 2013).

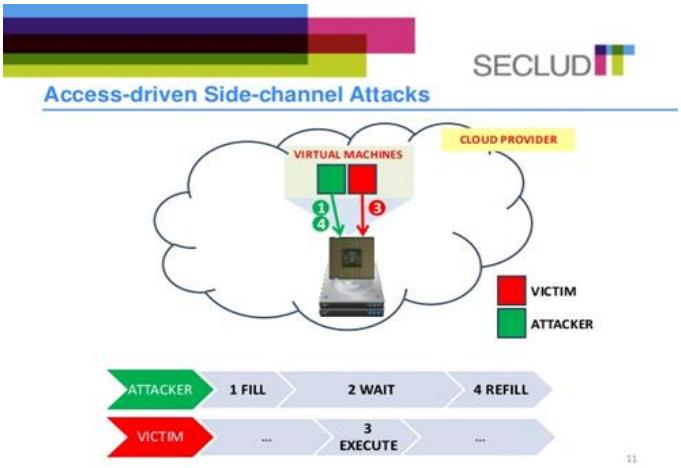


Figure 3: Side Channel Attack

3.3.1 Countermeasure of Side Channel Attacks

To protect side channel attacks on the server a combination of virtual firewall can be setup. A study shows that it is very possible to place a in close vicinity a malicious machine that would be indeed used to attack server later on. To tackle this a virtual firewall has to be setup. This firewall

prevents the attackers attempt of placing the malicious virtual machine during a side channel attack. Another approach to defend from side channel attack is to use the concept of confusion diffusion. By confusion it is meant to make a relation between the cipher text and plain text. Diffusion means to disappear the structure of plain text over bulk of cipher text. By using random decryption and encryption algorithms user data gets more protected and attacker faces more difficulties to crack the key (Godfrey and Zulkernine, 2013).

3.4 Authentication Attacks

In this type of attacks an intruder tries to get access to the authentication credentials used by a user to access cloud services. Authentication process with the advancement in technology day by day although have improved much from traditional login password phenomenon used before by various organizations. Currently such as secret question, shared mystery or number or picture selection to crosscheck human identity is also used before authentication process by various websites and applications.

- Brute Force Attacks are one of the most popular kinds of attacks to compromise system authentication. In this type of method an intruder infects tries all possible combination of passwords to break the security. These attacks are mostly done when the passwords are saved in encrypted form (Zunnurhain and Vrbsky, 2010).
- Dictionary Attacks can be said to be an enhanced version of Brute Force attack as it uses the same basics but unlike brute force attack it improves it efficiency by not checking all the combinations. A dictionary attack tries the most common words that are used in regular life in order to match the password (Zunnurhain and Vrbsky, 2010).
- Shoulder Surfing is a passive attack. It can also be said that this type of attack is carried by when someone's spying the user's actions in order to observe the keystrokes that are being typed on the keyboard (Zunnurhain and Vrbsky, 2010).
- Reply Attack is a network attack that is also said as reflection attacks. In this form of attacks, a valid authentication is delayed or the user authentication mechanism is challenged (Zunnurhain and Vrbsky, 2010).
- Phishing Attacks are a typical method to compromise user's authentication credentials. It uses a fake web page that looks exactly like the original one and when the user types in the sensitive information the attacker get is because it has the access to the webpage displayed to the user (Zunnurhain and Vrbsky, 2010).
- Key Loggers are spywares that make logs of each and every word that is being typed on the victim's keyboard. Via this the attacker can easily get access to the victim's sensitive information (Zunnurhain and Vrbsky, 2010).

3.4.1 Countermeasures of Authentication Attacks

A simple way of defending a brute force attack is giving intentional delayed responses. When provided with credentials to get logged in server delays before returning a response. This restricts the attacker to check too many combinations in a reasonable time (Zunnurhain and Vrbsky, 2010). Another approach to minimize authentication attacks is account locking. Accounts are locked for a brief period after incorrect login details provided. For example, account gets locked for an hour after 6 failed login attempts. This prevents attacker to check too many passwords together and takes a reasonable time (Zunnurhain and Vrbsky, 2010). Biometrics: is a newly developed technique in which a picture, finger prints or image could be used for the authentication process to make it more secure. The upside of this strategy is that it is genuine and one of a kind mark and can't be taken. The burden is that it is exorbitant and hard to execute. It's anything but a totally developed strategy and it very well may be effectively undermined and is tedious moreover (Fujita and Hirakawa, 2008).

3.5 Man-In-The-Middle

This is also a common type of attack that could be easily launched between the server and client by intruder over the internet. In this attack the attacker locates itself in between the two legit information sharers. Intercepts the messages during the public key exchange and retransmits them. The attacker must substitute its own public key for the requested one so the two legit end users won't know about the breech. In this process the two legit information sharers will appear to communicate normally (Raza et al., 2012). The message sender would not recognize that the receiver is not real but rather an assailant trying to access or modify the message before redirecting it to the intended user. This is how the attacker controls the whole communication. Some MIM attacks are:

- ARP or Address Resolution Protocol Communication. This protocol can be used by the attackers to conduct a MIM attack (Haataja and Toivanen, 2008). This protocol works to establish communication between two end devices in a network. The host PC broadcast an IP address and then a computer that has the same responds by returning its MAC address in it and then communication takes place. This protocol isn't a secured protocol and the attacker can easily benefit from it by responding with a forged MAC address to control the communication (Raza et al., 2012).
- Address Resolution Protocol Cache Poisoning: In this methodology the attacker sniff onto the network via controlling the network switch to monitor the flowing traffic in between the users. Attacker spoofs the packets between the sender and the receiver and does the MIM attack (Raza et al., 2012).
- Phishing or DNS spoofing. In this type of attack, the target will be provided with a fake web page created by the attacker that would be the identical copy of the original web page. When the user would provide its credentials thinking that it is a real web page its credentials will get to the attacker and then redirected to the actual site. The attacker will gain access to all the credentials (Raza et al., 2012).
- Attack can be carried out by stealing cookies of an already established session this method is known as session hijacking. Attacker can capture the requited parts of the session by capturing the cookies that were used in connection establishment between the host PC and the web server (Raza et al., 2012).

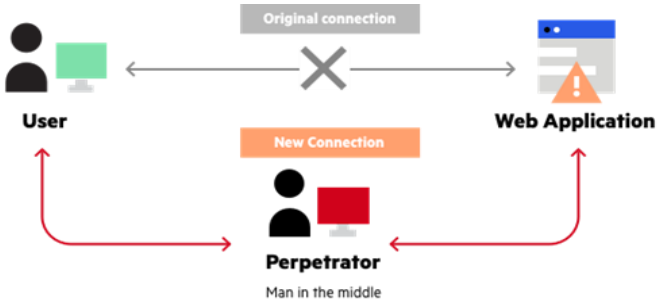


Figure 4: Man in Middle Attack

3.5.1 Countermeasure of MIM attacks:

To minimize MIM attacks one time passwords can be used because they're immune to MIM attacks.

By critically analyzing MIM attacks

- Host server's IP address
- Is the testament self-signed?
- Do other users on the inter have the same certificate?
- Is the certificate authenticated with certificate authority?

Cloud computing has security issue between client and server due to its open share issue between different customers and vendors by the service provider with common validation, the server checks the customer and the customer confirms the server to guarantee authentic correspondences are being traded. Check can be directed by utilizing open and private keys (Raza et al., 2012).

4. Open Issues / Challenges In Cloud Computing

The system is the foundation of Cloud, and henceforth vulnerabilities in arrange legitimately influence the security of Cloud. Security issues at arrange level ought to be considered as far as both outside and inward systems. A foe outside the Cloud arrange regularly performs DoS or DDoS assaults to influence the accessibility of Cloud administrations and assets. DoS/DDoS assaults decrease the data transfer capacity what's more, expands the blockage making poor help the clients. Due to the conveyed nature of the Cloud, it is difficult to avoid DoS/DDoS and Economic Denial of Sustainability (EDoS can be called as HTTP and XML based DDoS)

assaults (Subashini and Kavitha, 2011). Some normal assaults at the system layer are DNS harming assault, Sniffer assault, Port filtering, Cross site scripting, ARP parodying, IP mocking, and phishing assault, which are executed to get entrance of Cloud assets. Inner system assailant (approved clients or clients inside the cloud arrange) can without much of a stretch gain admittance to other client's assets without being recognized.

An insider has higher benefits and information (identified with organize, security component, and assets to assault) than the outside aggressor. Hence, it is simple for an insider to enter an assault than outside aggressors. Significant security issues at arrange level remember vulnerabilities for Internet conventions, approval, and confirmation, interruptions, secondary passage assault, session seizing, and clear information transmission. To address a portion of the issues at the system level, significant Cloud suppliers (like Amazon,Window Azure, Rack Space, Eucalyptus, and so forth.) are running their applications behind firewall. Be that as it may, it just gives security at limit of system and can't recognize the inner assaults. System based interruption recognition framework (NIDS) can be coordinated to address a portion of the security issues. Be that as it may, a NIDS ought to be designed for recognizing outer interruptions just as interior interruptions. It ought to likewise be equipped for distinguishing interruptions from encoded traffic. In the accompanying, we see the current research endeavors to address arrange security issues in Cloud.

Through trials and usage, the creators in studied about the security arrangements that can be applied to distinguish ARP caricaturing assaults (Zunnurhain and Vrbsky, 2010). They finished up that XArp apparatus is a productive security arrangement that can precisely identify ARP satirizing assaults (Raza et al., 2012). In a study we talked about existing NIDS ways to deal with Cloud (Haataja and Toivanen, 2008). For instance, a group researcher presented a grunt-based interruption discovery framework structure for Cloud system (Lo et al., 2010). As shown in Figure 5 an IDS module is installed on each region of cloud environment (Haataja and Toivanen, 2008). On the off chance that an interruption is distinguished at any district, it alarms different areas by utilizing a helpful operator. Different locales agreeably process seriousness of that and afterward separate it as an assault or ordinary movement dependent on an edge. This approach is appropriate for forestalling Cloud framework from single-purpose of-disappointment caused by DDoS assault. Be that as it may, it needs significant computational exertion.

Some researcher proposed a technique to verify VMs in Cloud from DDoS assault utilizing an IDS (Jensen, et al., 2009). In this methodology, Snort put together NIDS device is introduced with respect to the VM. On the off chance that any suspicious action is identified, it advises the source IP of that action and squares bundles originating from that IP. In the event that DDoS assault is discovered, it moves the administration running on influenced VM to another VM and hinders every one of the parcels. A group researcher displayed Snort based abuse discovery in open source Eucalyptus Cloud condition (Templeton and K. E. Levitt, 2003). In this methodology, Snort is conveyed at an essential controller overseeing cloud cases called cloud controller just as on the physical machines (facilitating virtual machines) to identify interruptions originating from outside systems. This methodology takes care of the issue of sending different occasions of IDS. In spite of the fact that it is a quick and financially savvy arrangement, it can just identify known assaults since just Snort is included.

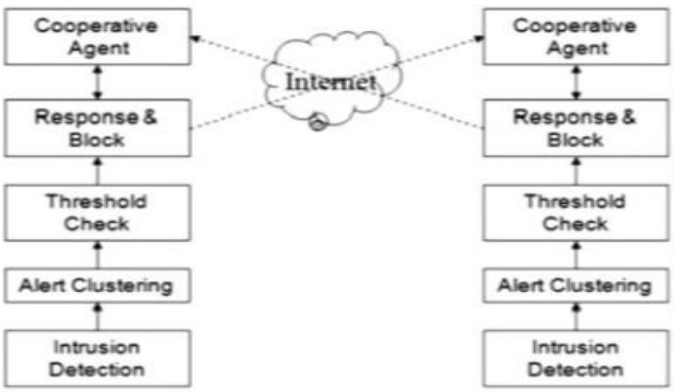


Figure 5: Limitations

A group researcher presented another sort of DDoS assault, called Economic Denial of Sustainability (EDoS) in Cloud benefits and proposed an answer structure for EDoS assurance (Godfrey and Zulkernine, 2013). EDoS assault can be called as HTTP and XML based DDoS assault. EDoS insurance structure utilizes firewall and confound server to identify EDoS assault. A firewall is utilized to distinguish EDoS at the section purpose of Cloud, though the riddle server is utilized to verify the client. In this work, the creators showed the EDoS assault in Amazon EC2 Cloud. Be that as it may, it's anything but an effective arrangement since it utilizes just conventional firewalls. Research is as yet expected to distinguish EDoS assaults in the Cloud.

To defeat impediments existing in above introduced approaches, further business related to NIDS is expected to give completely verify organize condition in the Cloud. Each other testing issue identified with the Cloud-NIDS is the observing and catching of the system traffic. This is expected to the multi-occupancy and circulated nature of Cloud figuring.

5. Conclusion

Cloud computing is a booming technology which is providing many advantages to different kind of establishments. But ensuring its privacy, security and user-trust are the main concerns of this technology as its security can be attacked and its functioning is affected by those attacks. For example, the different high-rate and the low-rate DDoS attacks destroy many of the features of the cloud computing, unauthentic user access can breach the data, and the other different attacks can be serious threats to the cloud environment. A cloud-computing environment delivering various services and hosting multiple resources can be protected if the resources are accessed only by the authenticated users. Strong authentication mechanism, restricting illegal resource-access, protecting cloud from authentication attacks and false or unauthentic users increases the security level of the cloud. It also includes description that the sources of the incoming packets are also certified in order to track down IP-spoofing by implementing active and passive Host-based OS finger-printing. While studying the attacks and prevention methods, it is demonstrated that many of the detection and prevention techniques of cloud-computing attacks have limitations. For example, hop count filtering can be used against IP-spoofing but is not useful to prevent other kind of attacks. The CBF method affects the accuracy because of static threshold and weight whereas the N-CBF method, which has dynamic threshold and weight, has better detection quality and is more accurate than the other techniques.

Future Work

Human computer interaction for validation and authentication process to be make more secure still allot of work could be done in this area to improve cloud security with less attacks in future. IDS; IPS etc. should be designed and used properly in cloud environment by the service providers.

References

Bhadauria, R., and Sanyal, S. 2012. Survey on security issues in cloud computing and associated mitigation techniques. International Journal of Computer Applications, 47–66.

Cheng, J., Wang, H., and K. G. 2003. Hop-count filtering: An effective defense against spoofed DDoS traffic. In Proceedings of the 10th ACM Conference on Computer and Communications Security (pp. 30–41). ACM.

Claycomb, W. R., and Nicoll, A. 2011. Insider threats to cloud computing: Directions for new research challenges. CERT. https://www.cert.org/archive/pdf/CERT_cloud_insiders.pdf

Fujita, K., and Hirakawa, Y. 2008. A study of password authentication methods against observing attacks. In Proceedings of the 6th International Symposium on Intelligent Systems and Informatics (SISY 2008).

Godfrey, M., and Zulkernine, M. 2013. A server-side solution to cache-based side-channel attacks in the cloud. In Proceedings of the IEEE Sixth International Conference on Cloud Computing (CLOUD) (pp. 163–170). IEEE.

Haataja, K., and Toivanen, P. 2008. Practical man-in-the-middle attacks against Bluetooth secure simple pairing. In Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2008) (pp. 1–5).

Jensen, M., Schwenk, J., Gruschka, N., and Iacono, L. L. 2009. On technical security issues in cloud computing. In Proceedings of the IEEE International Conference on Cloud Computing (pp. 109–116). IEEE.

Khorshed, M.T., Ali, A., and Wasimi, S.A., 2012. A survey on gaps, threat

remediation challenges, and some thoughts for proactive attack detection in cloud computing. Future Generation Computer Systems, 28(6), 833–851.

Lo, C.C., Huang, C.C., and Ku, J. 2010. A cooperative intrusion detection system framework for cloud computing. In Proceedings of the 39th International Conference on Parallel Processing Workshops (ICPPW 2010) (pp. 280–284). IEEE.

Luo, Q., and Fei, Y. 2011. Algorithmic collision analysis for evaluating cryptographic systems and side-channel attacks. In Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) (pp. 75–80). IEEE.

Perez-Botero, D., Szefer, J., and Lee, R.B., 2013. Characterizing hypervisor vulnerabilities in cloud computing servers. In Proceedings of the International Workshop on Security in Cloud Computing (pp. 3–10). ACM.

Raza, M., Iqbal, M., Sharif, M., and Haider, W. 2012. A survey of password attacks and comparative analysis on methods for secure authentication. World Applied Sciences Journal, 19, Pp. 439–444.

Subashini, S., and Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34 (1), Pp. 1–11.

Sumitra, B., and Misbahuddin, M. 2013. A survey of traditional and cloud-specific security issues. In Security in Computing and Communications (Communications in Computer and Information Science, 377, Pp. 110–129.

Takabi, H., Joshi, J. B. D., and Ahn, G.J. 2010. SecureCloud: Towards a comprehensive security framework for cloud computing environments. In Proceedings of the IEEE 34th Annual Computer Software and Applications Conference Workshops (pp. 393–398). IEEE.

Tang, H.Y., Siebenhaar, M., Miede, A., Huang, Y., Steinmetz, R. 2011. Threat as a service? The impact of virtualization on cloud security. IT Professional, 14(1), 32–37.

Templeton, S.J., Levitt, K. E. 2003. Detecting spoofed packets. In Proceedings of the IEEE DARPA Information Survivability Conference and Exposition, 1, pp. 164–175.

Tsai, W. T., Sun, X., Balasooriya, J. 2010. Service-oriented cloud computing architecture. In Proceedings of the IEEE Seventh International Conference on Information Technology: New Generations (ITNG) (pp. 684–689).

Varadharajan, V., Tupakula, U. 2013. Counteracting security attacks in virtual machines in the cloud using property-based attestation. Journal of Network and Computer Applications.

Zunnurhain, K., Vrbsky, S.V. 2010. Security attacks and solutions in clouds. In Proceedings of the 1st International Conference on Cloud Computing (pp. 145–156).