A Review On Various Attack Detection Techniques In cloud Architecture

Amandeep Kaur[1], Guide Name Anupama Kaur[2s]

ABSTRACT:-Cloud Computing Has been envisioned as the next generation architecture of the IT enterprise . Today's organizations, but there exist a many security vulnerabilities. Cloud Computing dynamically allocate, deploy, redeploy and cancel the services on the basis of demand . However, cloud computing inevitable posses a new challenges because traditional security mechanisms being followed are in sufficient to safeguard the cloud assests . Cloud Computing is easily can be targeted by the attackers. A group of malicious users or illegitimate users are attack on system and denial the services of legitimate users. Such kind of attacks are performed by the malicious(zombie) attackers. The zombie attack will degrades the network performance to large extend. There are various techniques described in this paper to isolate a zombie attack and other security vulnerabilities at cloud architecture.

Keywords:- Cloud Computing, Security, Zombie attack.

I. INTRODUCTION

Cloud Computing is a one of the emerging technology in sector where information is stored at the cloud servers by a customers including different devices like desktops , table computers , notebooks wall computers , sensors etc. Cloud Computing is a internet based computing which provides web services through service providers, these services are provided to the user on rent like pay-per-use model in which the user have to pay according to the access or use of the services With the arrival of this technology , the cost of computation , application hosting, contents storage and delivery is reduced significantly. Cloud computing is broken down into three segments " application", "platform", "infrastructure" and provide three types of services:-

(1) Infrastructure as a services:- Iaas provides a physical resources such as memory, processor etc.

(2) Platform as a service:- Paas provides the framework or platform on their own applications by using cloud and there is no need to install any platform on there own machine. Paas provides services such as .Net etc.

(3) Software as a service:- Saas is basically used for running the existing application like facebook .The user does not deal with installation of any software on their physical machine. The cloud provides such software for running these types of applications.

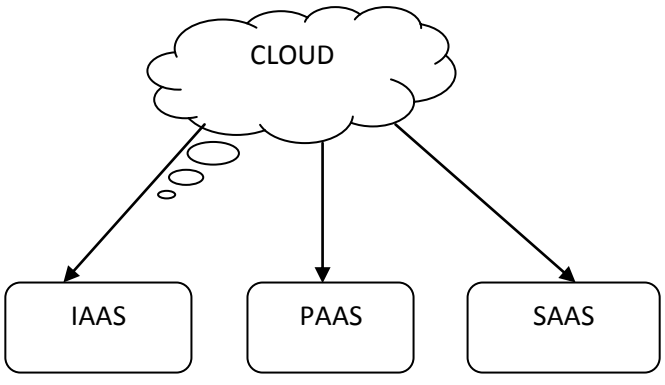

Fig:- 1 Cloud services

A Cloud can be a private or public or hybrid one. A public cloud can be accessed by anyone on the internet. A private cloud is a proprietary network

Amandeep Kaur[1], Deptartment CSE, Shaheed Udham Singh College of Engineering & Technology (Tangori), Mohali, India, +919779286588

Er. Anupama Kaur[2] , Deptartment CSE, Shaheed Udham Singh College of Engineering & Technology (Tangori), Mohali, India.

that provides the hosted to a limited number of people asking for the service. When a service provider uses a public cloud resources to create their own private cloud for their organizations, the combination of public and private cloud is hybrid cloud. Virtualization technology is another technology which goes along with the cloud environment which is used most widely to reduce the cost purchasing the hardware infrastructure in organization.

II Cloud Security

One and the major security issues in a cloud is to detect and prevent a network intrusion. There are the malicious users at client side, malicious user at cloud providers side and provider itself, can learn authentication information to gain a access of the others VMs. Malicious provider monitors network communication to gain information about client's behaviour. Cloud infrastructure makes a use of virtualization techniques, integrated technologies and run through standard internet protocols. These may attract a intruder due to many vulnerabilities involved in it. Cloud computing suffer from various traditional attacks such as zombie attack(flooding attack) and Denial of service attack etc. User can communicate with cloud service provider by a Virtual Machines and CSP manage the users data on a cloud at virtual servers. A illegitimate users or malicious attackers act as a legitimate users and affects the services of its legitimate users. There are some common intrusions , which causes availability, confidentiality and integrity issues to cloud resources and services.

a.Insider attack

Authorized cloud users may attempt to gain Unauthorized privileges. Insider may commit frauds and disclose information to others.

b.Flooding attack

Here, attacker tries to flood victim by sending huge number of packets from innocent host(zombies) in network. This type of attack may be possible due to illegitimate network connection.

c.Denial of service attack

In case of Cloud , the requests for VMs are accessible by anyone through internet, which may causes a Dos attack via zombies.

Flooding attack affects the service's availability on the intended service. Such an attack is called direct dos attack . For such kind of attacks signature based detection and anomaly detection techniques can be used. In a signature based detection a signature a priority algorithm is used. Where signature based detection is used for known attacks and anomaly is used for unknown attacks.

III LITERATURE SURVEY

Snehal G. Kene and Deepti P. Theng [12] It presents a review on intrusion detection techniques for cloud computing and security challenges. Cloud Computing is a 1st choice of every it organization because of its scalable and flexible nature. The security and privacy is a major Challenge in CC. IDS is most commonly used mechanism to detect a various attacks on cloud. In this paper Various IDS techniques are analyzed with respect to their types, positioning, detection time, detection techniques, data sources and attacks. The analysis provides alimitations of each technique to fullfill the security needs of cloud computing environment. R.Aishwarya & Dr.Sc Malliga[13] Proposed the intrusion detection system against DOS and DDOS attacks in the cloud environment . cloud computing is a one of the emerging and glooming technology in IT where information is permanently stored in the third party cloud servers and cached temporarily on clients with the help of different devices. One of the major threats to cloud security

is DOS or DDOS attack in the virtual machines. Here the DOS attack is overcome using hop-count filtering methodology. In the proposed method two layers of security are provided and MAC generator differentiates the legitimate client from the spoofed ones providing a security for the data packets allowing the clients to use the resources of the cloud server more efficiently. Fouad Guenane, Michele Nogueira and Guy Pujolle [14] . The Proposed technique is related to a reduction of DDOS attacks impacts using a hybrid cloud- based firewall architecture. This work presented a DDOS mitigation service based on hybrid cloud based architecture it provides a good performance in adopting existing technologies for the next generation of security services . As a future work it intend to study the impact of the proposed architecture on the application layer and design a better decision model. SS. Chopade, K. U. Pandey and D.S. Bhode [15]Securing cloud servers against flooding based attacks. This paper presents a simple distance estimation based technique to detect and present the cloud from flooding based DDOS attack and there by protect other servers and users from its adverse effects. Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee and Dijiang Huange (2013) [16] Propose the Network Intrusion Detection and Countermeasure Selection in virtual network system in cloud computing. Security from attacks is an important issue in a cloud computing & , attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large scale distributed denial of services. Dos attacks usually involve early stage actions such as multi-step exploitation, low frequency vulnerability scanning & compromising identified vulnerable virtual machines as zombies, with in the cloud system , especially the iaas clouds, the detection of zombie exploration attack is extremely difficult. For a better attack detection NICE employes a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, they preventing a zombie VMs. In this technique the (NICE-A) Network intrusion detection Agent is installed on each cloud server to capture and analyze the network traffic.The Proposed solution can significantly reduce the risk of the cloud system. NICE only investigates the network IDS approach to counter a zombie explorative attack . In order to improve the detection accuracy, host based IDS solutions spectrum of IDS in cloud system, This should be investigated in future work. Chirag N. Modi & Dhiran Patel (2013) [2] Propose a novel security framework hybrid network intrusion detection system. This framework aims to detect a network attacks in cloud by monitoring network traffic, while ensuring a performance and service quality. In H-NIDS two techniques signature Based detection for known attacks and anomaly detection techniques for unknown attacks are used. In signature based detection snort and signature apriority algorithm is used and in anomaly detection three different classifiers Bayesian, Associative & Decision tree are used. Moreover, a sutable score function determines whether the intrusion predicted by different classifiers are actually intrusion or not, Also it is used to detect a distributed attack in cloud.H-NIDS is deployed on each host machine in cloud. It helps to detect a internal & external network attacks. The central log and score function in H-NIDS helps to detect distributed attack in the cloud. Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez (2013) [1] Proposed the analysis of security issues of cloud computing. They worked up upon SPI model i.e SaaS,PaaS,IaaS) vulnerabilities and threats .As when data is travelled through internet or

involvement of third party is there, at that time we have to ensure the security factors and provide proof of security to organization. List of vulnerabilities and different threats, relationship between then is also discussed. Different types of virtualization technologies approach security mechanisms in different ways. Storage, virtualization, and networks are the biggest security concerns in Cloud Computing. They have focused on this distinction, where we consider important to understand these issues. Virtual networks are also target for some attacks especially when communicating with remote virtual machines.Due to some complexities in previous security mechanism it doesn't work properly because it was combination of different technologies, so new security techniques and technology is needed to avoid those problems. When virtual network communicate with remote virtual machines, it is also target for some security attacks and vulnerabilities. They have discussed some vulnerabilities and left with some for future work. Jian Yu, Quan Z. Sheng, Yanbo Han [3] Proposed special issues and service computing of cloud computing. Cloud services include reliability model, service virtualization, and user-centric services. Cloud service reliability mode l , service virtualization, and user-centric services. They have proposes a stochastic reliability model of atomic Web services. Some fault tolerance techniques have been proposed using recovery block adaptation to improve the quality of service. Fuzzy requirements and a two-level ranking algorithm are discussed and evaluated. One of them have proposes a spreadsheet-like programming environment called mashroom to support situational data integration by non professional users. This paper focus on key directions in this vibrant and rapidly expanding area of research and development. One important issue is that large-scale data centers must offer reliable and secure services with high quality standards to satisfy the on-demand needs of users, to develop service security. Joel Gibson, Darren Eveleigh, Robin Rondeau, Qling Tan [2]: Proposed the challenges that are faced by the service models in cloud. The three pre dominant models that are present in the cloud computing are mainly infrastructure as service, platform as service and software as service. Infrastructure as service provides with the use of servers, storage and virtualization to enable utility like services for user. Security becomes the major challenge in the infrastructure as service as rest of the top cloud services run on the top of this service In software as service and platform as service the major challenge that arises is that at times it becomes critical to understand the cloud service models which determine the cloud services hosting are an appropriate business solution.This paper gives clear indication that services should be available at anytime and anywhere so that availability of services do not decrease. Main issue is lack of services and resource availability which leads to inadequacy. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom [4]: Proposed the research related to security of single cloud and multi-cloud and solution regarding them. As dealing with single cloud became less popular, due to innovation of "multi-cloud", "intercloud", "cloud of cloud". Various security factors have different impacts on different services. As its being described that multi-cloud infrastructure requires less security attention as compare to single cloud. Recently several users faced many problems due to data intrusion, availability. Security techniques such as encrypting data using cryptographic hash function for maintaining data integrity and storing data on different servers to overcome the limitation of availability of data. For virtual storage Depsky data model which deals with different cloud

provider is a being used with depsky library. Byzantine protocol which deals with hardware and software faults called as byzantine faults. Limitation of encryption is that encrypted data can't be manipulated. However use of multi-cloud due to ability to decrease security risks will also affect user involved in cloud computing environment.

IV Problem statement

Cloud computing inevitably poses new challenging security threats for number of reasons. Firstly, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including modification, insertion, deletion, appending and reordering, etc. To ensure storage accuracy under dynamic data update is most importance.

However this dynamic feature also makes traditional integrity insurance techniques futile and entails new solutions. In the previous times various effective distributed technique with overt dynamic data support to ensure that of users data in the cloud is correct. They depend on Elimination correcting code in the file distribution preparation to provide redundancies and guarantee in the data dependability. This design reduces the communication and storage overhead as such as the traditional replication based file distribution scheme. By using the homomorphic token with distributed verification of erasure coded data and their scheme achieves the data correctness insurance and data error localization whenever data corruption has been identified during the storage correctness verification their method can almost guarantee the simultaneous localization of data errors, i.e., the detecting the misbehaving server(s). The new method further supports secure and efficient dynamic operations on data blocks including: deletion data update and append. Extensive performance and described security analysis shows that the proposed technique is highly efficient and resilient against Byzantine failure, malicious data altering attack and even denial of services attacks also. In future work, we propose a novel technique to isolate zombie attack in cloud architecture and tried to detect a malicious attackers with secure authentication between user and server.

V EXISTING TECHNIQUES

International data corporation (IDC) survey showed that security is the biggest challenge in cloud computing. The recent cloud computing security white paper by Lockheed Martin Cyber Security division shows that the major security concern after data security in intrusion detection and prevention in cloud infrastructure, Cloud infrastructure makes a use of virtualization techniques, integrated technologies and run through standard internet protocol. These may attract intruders due to many vulnerabilities involved in it.[9] Cloud computing also suffer from various traditional attacks such as insider attacks, flooding attack . Firewall can be a good option to prevent outside attacks but does not work for insider attacks. Efficient intrusion detection and intrusion prevention systems should be incorporated in cloud infrastructure to migrate these attacks. Traditional

IDS/IPS such as signature based detection and anomaly detection. Signature based detection is an efficient solution for finding known attacks but fails to detect unknown attacks or variations of known attacks. SNORT is a tool used to detect a such kind of attacks. Anomaly detection technique is used at cloud to detect a unknown attacks at different levels. This technique is proposed to detect a intrusion at different layers of cloud.[10] NIDS is network intrusion detection system technique in this both signature based detection and anomaly detection techniques are available. In this technique snort is used filter the known attacks from the captured network traffic and then apply a classifier to detect a network anomaly. These techniques can efficiently detect as well as unknown attacks but rare some challenges in this technique.[11] H-NIDS is a hybrid network intrusion detection system . in this technique sensor on each host machine to monitor and detect the network intrusion in cloud environment. In this both signature and anomaly detection techniques are used but in anomaly three classifiers are used. Moreover score function is used to determine whether the intrusion predicted by a different classifiers are actually intrusion or not. Also it is used to detect a distributed attack in cloud. But some times it generates a false alert.[12] There are many techniques to detect attacks but there exist some vulnerabilities. In this paper various techniques and security vulnerabilities studied to provide a security at cloud architecture from malicious attackers . In future work propose novel technique with cryptography based scheme to isolate zombie(malicious attacker) and detect a malicious virtual machine in cloud architecture..

CONCLUSION

Cloud computing incorporates on-demand deployment, virtualization, open source software, and Internet delivery of services . The Cloud Computing Architecture which contains on-premise and cloud resources, middleware, , services, and software components, geolocation, the externally visible properties of those and the relationships between them this is also refers as documentation of a system's cloud computing architecture. Due to this mobility increases and employees can access the information anywhere. There is capability of cloud computing to free-up IT workers who may have been occupied to performing factions like , installing ,updates and patches or involving in application support. As good services and benefit of Cloud Computing has to provided but there are security issues which make users unstable about the efficiency, safety and reliability in cloud computing. The zombie attack will degrades the network performance to large extend. In future work, new technique will be proposed which isolate zombie attack and detect malicious VM machines are responsible to trigger zombie attack with the help of mutual authentication scheme.

REFERENCES

[1] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez (2013) *"An analysis of security issues for cloud computing"*2013

[2] Jian Yu, Quan Z. Sheng, Yanbo Han (2013) *"Introduction to special issue on cloud and service computing"* 26 April 2013

[3] Joel Gibson, Darren Eveleigh, Robin Rondeau and Qing Tan (2012) *"Benefits and Challenges*

*of Three Cloud Computing Service Models"*2012 IEEE

[4] Mohammed A. AlZain #, Eric Pardede #, Ben Soh #, James A. Thom* (2012*) "Cloud Computing Security: From Single to Multi-Clouds"* 2012 45th Hawaii International Conference.

[5]Anas BOUA Y AD, Asmae BLILA T, Nour el houda MEJHED, Mohammed EL GHAZI (2012) "*Cloud computing : security challenges"*2012 IEEE.

[5] Ravi jhawar, Vincenzo Piuri,Fellow,and Macro santanbrogio(2012)*"Fault tolerance management*" 2012 IEEE.

[6] Mohamed Hamdi(2012) "*Security of Cloud Computing, Storage, and Networking***"** 7/12.2012 IEEE

[7] Huaglory Tianfield(2012) *"Security Issues In Cloud Computing***"** 2012 IEEE October 14-17, 2012.

[8] International Data Corporation. 2009.[Online].Available: http://blogs.idc.com/ie/wpcontent/uploads/2009/12/idc_cloud_challenge s_2009.jpg, 2009.

[9] Modi, C., Patel, D., Patel, H., Borisaniya, B., Patel, A. & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. Journal of Network and Computer Applications, 36(1), pp. 42-57. doi: 10.1016/j.jnca.2012.05.003 http://dx.doi.org/10.1016/j.jnca.2012.05.003

[10] C. N. Modi. D. R. Patel. A. Patel, and R . Muttukrishnan, "Bayesian Classifier and Snort based Network Intrusion Detection System in cloud computing," International conference on Computing, Communication and networking technologies(ICCCNT-Coimbatore), IEEE, 2012.

[11] C. Modi, D, Patel, b. Borisanya, A. Patel, an," M. Rajarajan," A novel framework for intrusion detection in cloud ,"Proceeding of the Fifth International Conference on Security of Information and Networks(SIN-2012), 2012, pp, 67-74.

[12] Snehal G. Kene and Deepti P. Theng (2015), " A Review on intrusion detection techniques for cloud computing and security challenges" , IEEE 2014 .

[13] R.Aishwarya & Dr.Sc Malliga(2014) , "IDS – An efficient way to thwart against DOS/DDOS attack in cloud environment", IEEE 2015.

[14] Fouad Guenane, Michele Nogueira and Guy Pujolle (2014) ," Reducing the DDOS attacks impacts using hybrid cloud-based firewalling architecture", IEEE2014.

[15] S.S. Chopade, K. U. Pandey and D.S. Bhode (2013), "Securing a cloud servers against flooding based DDOS attacks", IEEE 2013.

[16] Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee, and Dijiang Huang (2013), "Network Intrusion detection and countermeasure selection in virtual network systems ", IEEE (2013).

