International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

Security mechanism against malicious attacks from intruders in cloud computing environments

Chikram Sridhar[1], Ramesh Polisetti[2] , M.Rakesh Chowdary[3]
[1]Assistant Professor, Department of CSE
[2]Assistant Professor, Department of CSE
[3]Research Scholar at Satyasai University of Technological & Medical Sciences, Bhopal, M.P.
[1,2,3]Sree Datha Group of Institutions

Abstract: Cloud computing is a booming internet driven technology, which renders a pool of resources such as network, storage, and applications on-demand basis. The cloud Services must be highly secured so that it increases the adoption of cloud for enterprise business management. The cloud services are shared by multitenant using internet channel which is a vulnerable to attacks. Cloud computing is exposed to many threats**.** This paper discusses different techniques and extends with the issues such as challenges, security attacks, DDoS attacks and intrusion detection methods. Cloud computing allows huge volume of storage on web which makes available the data and services in distributed environment. Intruders target the cloud based data due to its storage nature. The most famous attack of cloud computing is Distributed Denial of Service (DDoS) attack. The DDoS is the biggest threat in the areas of internet and internet of things (IOT). To prevent these kinds of attack, the intrusion detection system should have strong protective mechanism.

Keywords- Cloud computing security attacks, DDoS attacks, Intrusion detection systems

I. INTRODUCTION

In the field of computation, there have been many approaches for enhancing the parallelism and distribution of resources for the advancement and acceleration of data utilization. Data clusters, distributed database management systems, data grids, and many more mechanisms have been introduced. Now cloud computing is emerging as the mechanism for high level computation, as well as serving as a storage system for resources. Clouds allow users to pay for whatever resources they use, allowing users to increase or decrease the amount of resources requested as needed. Cloud servers can be used to motivate the initiation of a business and ease its financial burden in terms of Capital Expenditure and Operational Expenditure. There are many questions that arise as to whether a cloud is secure enough. Considering malicious intruders, there are many kinds of possible attacks, such as a Wrapping attack, Malware-Injection attack, Flooding attack and Browser attack. A Wrapping attack is done by duplication of the user account and password in the log-in phase so that the SOAP (Simple Object Access Protocol) messages that are exchanged during the setup phase between the Web browser and server are affected by the attackers. In a MalwareInjection attack, the attacker creates a normal operation, such as delete User, and embeds in it another command, such as setAdminRight. So, when the user request is passed to the server, rather than the server executing the command as if it were deleting a user account, it actually discloses a user account to the attacker. A Flooding attack occurs when an attacker generates bogus data, which could be resource requests or some type of code to be run in the application of a legitimate user, engaging the server's CPU, memory and all other devices to compute the malware requests. The servers finally end up reaching their maximum capacity, and thereby offload to another server, which results in flooding.

II. RELATED WORK

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 a limitations of each technique to fulfill 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 suitable 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 an 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, Yanbu 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 nonprofessional 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 major0 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 ardede, 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

III. SUGGESTED ARRANGEMENTS

Intrusion Detection Systems (IDS) are indispensable part of securing cloud data in distributed environment. The primary goal of IDS is used here to detect intrusion behavior from malicious host or network and attain appropriate response. IDS is mainly categorized into two types, they are network based and host based. The prominent feature of IDS is to provide unusual activities by sending notification alert to the administrator to block distrusted connection and also able to distinguish among intruders from inside the organization (threat posed by insiders) and from malicious hackers [14]. Intruders can use a variety of attacks to make use of cloud systems, they are,

- DDoS attack
- Insider attack
- Hypervisor level attack
- User to root attack
- Backdoor channel attacks
- Port scanning
- Flooding attack
- Virtual Machine level attack (VM)

Intrusion Detection System types

There are various types of intrusion detection methods are used in cloud computing.

Host-Based Intrusion Detection System (HIDS):

Host based intrusion detection system is a software which monitor the host machine and sends an alert when a distrustful event occurs. This type of IDS is used to collect all the incoming and outgoing packets traffic from the user terminal. To detect anomalous behaviors, HIDS software can be installed in hypervisors or virtual machines to inspect log files and access control policies.

Network-Based Intrusion Detection System (NIDS):

Network based intrusion detection system monitors network traffic and network packets to detect attacks. In a network, number of host machines are connected and analyzed, NIDS is responsible for listening and defending the network segments. NIDS has the most powerful mechanism to detect network intruders by creating real time comparison and it overcomes the drawbacks of Host based IDS. Cloud server use network IDS on the virtual machine or hypervisor to monitor network packets log and protect from suspicious activity [15]. Cloud provider is only responsible for deploying NIDS in the cloud environment and the major drawback is that any attack happens outside the supervisor there is no guarantee to the data.

Hypervisor Based Intrusion Detection System:

Hypervisor based intrusion detection system runs on Hypervisor Layer. Virtual machines are created and executed by hypervisor, each virtual machine in a network is called guest machine. Here network communications are monitored between VMs, Hypervisor and VM, and within the hypervisor. Hypervisor based IDS maintains higher data availability in the cloud server and in the virtualized cloud environment, it contributes more to protect, analyze, and detect malicious intruders [15]. Example of hypervisor based intrusion detection is Virtual machine introspection based IDS (VMI-IDS).

Distributed Intrusion Detection System:

Distributed Intrusion Detection System has numerous IDS in a large network connection, which uses host based and network based IDS's. Every single Intrusion detection system communicates each other and central server for monitoring activities. DIDS is appropriate mechanism for Cloud based attack detection and log maintenance. In the cloud environment, DIDS works on host machine or processing server database, and different IDSs gather data from network and host system and convert them

to standard format. As a final point, centralized analyzer get the standard format of data from IDS [16].

Network Behavior Analysis Intrusion Detection System: Network behavior analysis (NBA) is a process of improve the protection of a network by supervising unusual traffic flows and observing abnormal actions, such as DDoS attacks, some category of malwares, and strategy violations. DDoS attack is an essential security risk to internet service vendors and large network infrastructures. Based on the network behavior, threats can be identified and maintain the log file.

Intrusion Prevention System (Inline Security System): Intrusion Prevention System (IPS) is used to prevent the system from threats and observe the network traffic. When a system is vulnerable, the attackers attempt to inject malicious code to the targeted application and get control of an application. IPS (Active system) is advanced and more efficient method of IDS (Passive System). It has direct communication pathway among source and destination, so that system actively monitor the network traffic and take action according to that, such as

- Sends an alarm signal to the admin
- Avoid suspicious packets
- Jamming network disruption from the starting address

Refresh the connection

Intrusion detection techniques

Pattern-Based Intrusion Detection: Pattern based detection is also known as Signature based detection, which detects threats based on the predefined pattern but does not detect latest threats since it does not hold updated recent patterns. This pattern based approach is used in host and network based IDS to monitor the malicious behavior.

Anomaly-Based Intrusion Detection: Anomaly-based intrusion detection is used to detect anomalous, unusual (abnormal) attacks using existing behavior pattern. Existing behavior of the user, host, and network connections over the period of time can be taken and stored in the database; anomaly detectors gather normal or usual data which gives normal behavior. This intrusion detection system detects and gives alarm automatically with the help of existing usual behavior data. IDS has ability to find new types of errors without modifying existing data using Threshold detection, Statistical analysis, Rule based measures, Neural networks, and Genetic algorithms. One disadvantage observed in this system is that to make effective IDS, it needs accurate updating of behavior data.

IV. CONCLUSION

Cloud computing backbone is distributed platform on the other side expect large number of security measures and subsequent weaknesses in a system. This paper provides comparative study on various security attacks in the Cloud environment, impact of DDoS attacks and intrusion detection systems. DDoS attack is most challenging one for the users to access cloud resources.

REFERENCES

[1]. Tao Peng, Christopher Leckie, Kotagiri Ramamohanarao, “Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems”, ACM Transactions on Computational Logic, Vol. 2, No. 3, 2006.

[2]. M. Durairaj, P. Kannan, “A Novel Approach for Elastic Application Partitioning in Mobile Cloud”, IEEE - ICAET-4th International Conference on Advances In Engineering & Technology, India, 2014.

[3]. M. Durairaj, P. Kannan, “A study on Virtualization Techniques and Challenges in Cloud Computing”, International Journal of Scientific &Technology Research, Volume 1, Issue 1, 2014.

[4] Mohammed A. AlZain #, Eric Pardede #, Ben Soh #, James A. Thom* (2012) “Cloud Computing

Security: From Single to MultiClouds" 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.

[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_challenges_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.

Authors:


Chikram Sridhar working as Asst. professor with 2 years of experience at Sree Datha Group of Institutions.


Ramesh Polisetti working as Asst. professor with 2 years of experience at Sree Datha Group of Institutions.


M.Rakesh Chowdary Research Scholar at Satyasai University of Technological & Medical Sciences, Bhopal, with teaching experience of 5 years at Sree Datha Group of Institutions.