A Survey on Denial of Service Attack Detection Techniques in Cloud Computing

Reena Singh Rajput[1] Dr. Sanjay Agrawal[2]
[1]Student [2]Professor
[1,2]Department of Computer Technology & Application
[1,2]NITTTR, Bhopal, India

Abstract— Cloud computing is technology that enables the clients to get access to the services and resources according to their demand. Cloud Computing is on-demand and self-service in nature. The main concern in Cloud Computing is security. There are numerous threats, attacks and security problems in cloud. Most concerning security threat is DOS, which is the single largest threat to internet and internet of things. Denial of Service (DOS) is an attempt to create the resources and services inaccessible to the legitimate users by flooding network with a many requests. This paper contains a survey on DOS Attack and its detection techniques in cloud computing environment. Cloud security is great concern therefore care should be taken to provide secure cloud and secure, uninterrupted cloud services.

Key words: Cloud Computing, Denial of Service (DOS), Attacks, Security, Related Work and Techniques

I. INTRODUCTION

Cloud computing is internet based computing and it is one of the most important technologies that provide flexible, cost effective, pay on used basis services like huge storage, computing power and many other over internet. As these all services are outsourced i.e. provided by the third party, they have increased the risk of maintaining data security, data privacy, supporting the services and data availability all the time. Some definitions of cloud computing are given below:

"A large-scale distributed computing paradigm that is driven by economies of scale, in which a pool of abstracted virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered on demand to external customers over the Internet [1]".

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." - National Institute of Standards and Technology (NIST) [2].

Cloud offers services in 3 levels specifically infrastructure, platform and software system to satisfy the requirements of various types of customers. The key cloud characteristics embody multi-tenancy, location and device independence, elasticity, resource pooling and measured service. The IT corporations particularly the small and Medium Scale Businesses are moving onto the cloud that allows them to perform high end computational tasks in an exceedingly price effective manner.

IT organisation will be provided as a service in cloud, security becomes a serious concern. Among the many attacks which will target the cloud environment, DoS or DDoS attacks cause a serious breach in security. Security is the major concern in Cloud Computing. One of the most important security problems is DOS, i.e. the one largest threat to internet and internet of things.

A. Cloud Computing Security

Cloud security is a major area of concern when dealing with a cloud. Security is one of the main concerns when it comes to any kind of technology and so is important in cloud. There are various kinds of security breaches which are present. Security breaches like denial of service attack (DoS) or man in the middle attack not only affects the performance of cloud but also makes the cloud less reliable and affects it's services. The next section defines the security principal, and threats to cloud computing systems.

B. Cloud Computing Security Principals

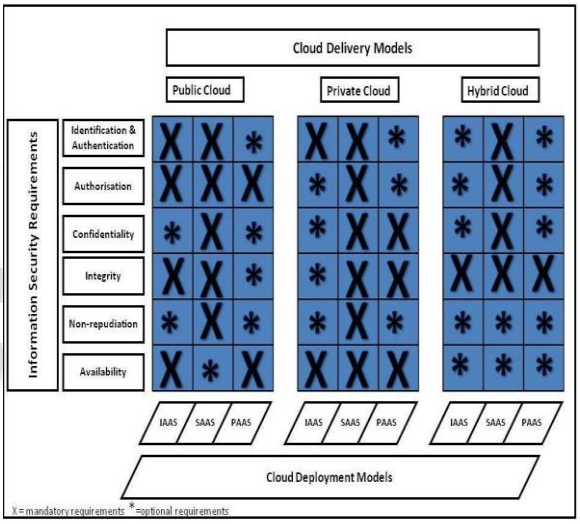

Fig. 1: Cloud Computing Security Requirements [18]

Ramgovind, Eloff, & Smith defined six cloud computing security principles [18]:

- Identification & Authentication: Here we identify the users requesting access and their checks priorities, then after see the permissions.
- Confidentiality: Confidentiality is a basic requirement that control and maintain data that are distributed different location in different organization. In public cloud confidentiality is must.
- Integrity: The integrity of information which requires Atomicity, Consistency, Isolation And Durability (ACID) properties must be enforced across all cloud computing delivery models.
- Non-repudiation: Security protocols and token provisioning for data transmission, such as using digital signatures, timestamps and confirmation receipts services, should be applied to maintain non-repudiation.
- Availability: When choosing among private, public or hybrid cloud vendors and making further decisions concerning delivery models, availability factors for the

different vendors must be considered. The illustration below in figure 1 shows a visual representation of the information presented above for different configurations.

II. DIFFERENT SECURITY ATTACKS OF CLOUDS

There are many attacks possible on cloud. Some examples are mentioned below

A. *Denial-of-Service Attack (DoS)*

Cloud is penetrable to DOS attacks, because so many users are using the cloud services and resources, so DOS attacks can cause a lot of damage. "A DoS attack is like being caught in rush-hour traffic gridlock , there's no way to get to your destination, and nothing you can do about it except sit and wait" [13].

Distributed denial of service (DDoS or DoS) occurs to a server when attacker sends a large amount of fake request packet from a many of zombie computers that are already under the control of attacker. DDoS have become a serious problem and the attackers are using so many ways to target the victims. Many defence mechanisms have been proposed to avoid and detect DDoS attacks [9][10].

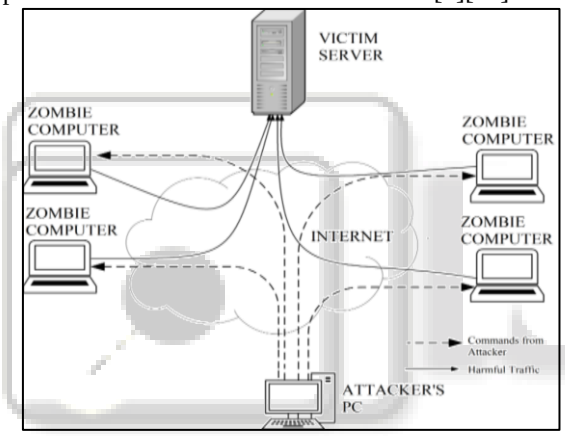

Fig. 1: DDoS Attack [11]

Another type of the DoS attacks are smurf attack, UDP Bombing, TCP Syn Flooding, Ping of Death, HTTP based DoS Attack (HDoS), XML based DoS Attack (XDoS) etc.

B. *Cloud Malware-Injection Attack*

It is the primary considerable attack that attempts to inject implementation of a malicious service or virtual machine into the Cloud. The aim of cloud malware can be anything that the adversary is interested in, it may embrace data modifications, full functionality changes/reverse or blocking. During this attack adversary creates its own malicious service implementation module (SaaS or PaaS) or VM instance (IaaS), and add it to the Cloud system [8]. The term Malware also includes Worms, Trojan Horses, Rootkits, Spyware, Adware, Crimeware, Robot (botnet) Clients etc [3]. Some activity of Malware Injection attack are as below [3]:

- Degraded the performances of computer operations.
- Intrusive pop-up windows.
- Spam email creating unwanted products, services or activities these is distasteful or illegal.
- Larceny of personal, financial or corporate data.

C. *Side Channel Attack*

In side-channel attacks, the attacker runs a VM on an equivalent physical host of the victim's VM and takes benefit of a shared physical part (e.g. the processor cache) in order to steal information (e.g. a cryptographic key) from the victim. Side-channel attacks have egressed as a form of effective security threat targeting system implementation of cryptographic algorithm [3][8].

D. *Man in Middle Attack*

Lack of TLS certificate validation, permitting an attacker to eavesdrop and even modify calls and text messages [13]. This attack happens when an attacker put himself between two users. Anytime attackers can place themselves in the communications path, there are chances that attacker may intercept and modify communications [8].

E. *Replay Attack*

The authenticate data may be used in maliciously or fraudulently [13].

F. *Port Scanning*

Intruders may seize information with the help of open ports like services that run on a system, IP and MAC addresses those belong to a connection, and router, gateway and firewall rules. TCP, UDP, SYN/FIN/ACK and Window scanning. [13]

III. RELATED WORK AND TECHNIQUES

In this section different DoS attack detection and prevention techniques for cloud computing proposed by different authors are discussed.

A. *Securing Cloud Servers against Flooding Based DDOS Attacks*

S.S. Chopade, et.al.[6] The author has proposed an easy distance estimation based technique to detect and prevent the cloud from flooding based DDoS attack and there by defending alternative servers and users from its adverse effects. In this paper, author has used a distance-based DDoS technique that uses an easy however effective exponential smoothing technique to predict the average of distance within the next period. The proposed technique depends on MMSE to support efficient traffic arrival rate prediction for separated traffic. Author has checked the technique in the Internet-like network enforced on NS2 with over a hundred nodes. The experimental results show that the proposed technique is effective and may observe DDoS attacks with high detection rate and low false positive rate.

B. *Securing Cloud Computing Environment against DDoS Attack*

Joshi, Bansidhar et.al. [7] The author used Cloud Trace Back (CTB) model for detecting DDoS attacks using back propagation neural network. The system handles DDoS attack. Main architectural idea behind CTB is the use of Services Oriented Architectural (SOA) method to Trace Back methodology, for finding source of a DDoS. Deterministic Packet Marking method is used by CTB. In the proposed work, the CTB uses FDPM by incorporating the cloud trace back mark (CTM) within the Cloud trace back header in the web service message. Each request sends to the CTB header for marking then after the sender's

address is removed that increases the security. If, the attack is occurred then the victim can recover and reinitialize the CTM tag that reveals the source of the attack. This technique introduces the use of a back propagation neural network which is called Cloud Protector. Cloud Protector is trained to detect and filter attack traffic. The system detects attacks in a very short period of time and can successfully trace back 75-81% of the attacks.

C. A Packet Marking Approach to Protect Cloud Environment against DDoS Attacks

E.Anitha et al. [16] author has proposed a new technique for detection of DDoS attack employing a packet marking approach. In this technique HX-DoS attacks square measure checked against cloud web services to discriminate between the legitimate and illegitimate messages. This can be through with the assistance of rule set based detection, known as CLASSIE. The author is employed modulo marking technique for avoiding the spoof attack. Reconstruct and Drop technique is employed on the victim aspect to drop the packets and take decision. The proposed technique improves the reduction of false positive rate, detection and filtering of DDoS attacks.

D. A Packet Filtering Method for DDoS Attack Defense in Cloud Environment

Qi Chen et.al [12] author has proposed an approach works on 2 phases particularly a non-attack phase and an attack phase. During a non-attack phase, it identifies distinctive correlation patterns among legitimate packets by extracting attribute pairs in their IP and TCP headers. Then it calculates a confidence value to find the trustworthiness of a specific correlation pattern between an attribute pair. Maximum the frequency of an attribute pair during normal packet flow, Maximum confidence value it will get. This dataset called nominal profile. In attack phase, CBF score for every packet is calculated that is the weighted average of confidence values of attribute pairs in it. Then the CBF score is compared with discarding threshold to choose whether the packet is legitimate or not. If CBF value is over the threshold, the packet is legitimate and allowed to pass instead the packet is discarded. The merits of CBF methodology includes less storage space, high computational speed and efficiency that makes it appropriate for large network traffic.

E. Defense against DoS Attack: PSO Approach in Virtualization

S.Mercyshalinie et.al. [17] Author has proposed the framework to detect and mitigate TCPSYN flood attack. For this purpose, it developed the defense problem as an optimization problem that tries to reduce numbers of rejected connection requests and to reduce share of attack half-open connections from the TCP memory space. This solution led to a self-securing server that frequently monitors some performance metrics then tries to increase the security degree by dynamically setting of the desired parameters. Theoretical analysis show that the proposed solution gives an optimal value .The proposed defence mechanism improves performance of the under attack server. This defence mechanism show that h and m are effective control points to safe the TCP servers against SYN flood attack.

F. Exploiting Artificial Immune System to Detect Unknown DoS Attack in Real Time

Dawei Wang et.al [14] the author has proposed a flow-based DOS detection system based on Artificial Immune systems. It adopts a tree structure to store flow info such that we are able to effectively extract useful features from flow info for higher detecting DoS attacks. Author employs Neighborhood Negative selection (NNS) as the detection rules to detect unknown DoS attacks, and determine attack flows from large traffic. As a result of the robust tolerance Identify of NNS, the proposed solution is able to quickly get attack dynamics. The experimental results show that this solution is able to effectively find unknown DoS attack flows and determine attack flows from background traffic. The weakness of this paper it doesn't find all form of dos attack.

G. Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach

MohdNazri et.al. [15], the author has proposed a new model to detect flooding based DoS attack in cloud computing. The primary part concerns normal traffic pattern for baseline profiling, whereas the next part is intrusion detection processes followed by the prevention part. The covariance Matrix mathematical model is employed as a detecting technique. The primary part and second part have been implemented in real test bed. From the result, it is proven that can be detected the flooding attack effectively.

H. Analysis and Detection of DoS Attacks in Cloud Computing by using QSE Algorithm

PallavaliRadha et al. [13] the author has proposed a way for detection of DoS attack in Cloud by Quantum Swarm evolutionary algorithm. The authors used quantum inspired particle swarm optimization for analyze and detect the DoS attack in cloud. The proposed system was divided into 3 steps-basic feature selections for individual records, QSE working nature and decision making. Anomaly based mostly detection technique is employed for decision making as a result of it finds any kind of DoS attack while not having any information regarding the attacker. The complete technique is split into 2 sub-phases particularly training and testing. The training part, normal traffic is captured and so QSE algorithm is enforced during this part for generating normal traffic profile. The testing part, QSE module is employed for detecting abnormal traffic. The ascertained outcomes were compared with QEA algorithm and QSE was found to be higher than QEA.

S. No.	Method	Features	Limitations
1	Distance estimation based technique (MMSE)	– High detection rate. – Low false positive rate.	– Does not detects all type of denial of services attacks.
2	Cloud Trace back Model	– Averts direct DDoS with CTB. – Identity of attacker will be made	– Collecting proper training data set for neural network is difficult.

		known during successful DDoS attack.	– Performance depends on accuracy of training data set.
3	Confidence Based Filtering Approach	– Small storage size for nominal profile and high packet filtering efficiency. – Reduce computational speed.	– Does not have high accuracy than other approaches.
4	CLASSIE Packet Marking Approach	– Identifies HX-DoS attacks 2.Reduces false positive rate of DoS attacks	– Helps to identify only application layer DDoS attacks.
5	Covariance matrix approach	– Detect the flooding attack effectively	– Does not high accuracy than other approaches
6	Artificial Immune systems (NNS)	– Detects the DoS attacks within a very short period of time.	– It doesn't find all form of DoS attack

Table 1: Summary of approaches to Denial of services attacks in cloud.

IV. Conclusion and Future Work

This paper has reviewed different type of security attacks that affect the performances of cloud security. The Denial of services attack (DoS) and Distributed denial of services attacks are major threats to cloud security. Here, the authors have discussed DoS detection techniques as well as presented a comparative analysis of these detection techniques. After study of these techniques it was found that there are a lot of methodologies and tools devised to detect DoS and DDoS attacks that can help to overcome the damage they cause. Still we are far from efficient detection of DoS detection with a small number of false alarms and real-time transfer of packets.

In future work the authors propose to use Swarm intelligence algorithms for detection of DOS attack. Use of swarm intelligence techniques to detect the DOS attack can improve the overall security in cloud computing. It can bring the stability and reliability in the Cloud network and its early detection can prevent the network from going down.

References

[1] Foster, Ian, Yong Zhao, Ioan Raicu, et al, "Cloud Computing and Grid Computing 360-Degree Compared", In Grid Computing Environments Workshop (GCE), Austin, 2008
[2] Zhou, R. and K. Hwang et.al "Trust-Preserving Overlay Networks for Global Reputation Aggregation in Scalable P2P Systems", IEEE transaction on Parallel and Distributed Systems, (TPDS), revised March 2006.
[3] IR.Ramya, IIG.Kesavaraj et.al "A Survey on Denial of Service Attack in Cloud Computing Environment" International Journal of Advanced Research in Education & Technology (IJARET) Vol. 2, Issue 3 (July - Sept. 2015)
[4] Meiko Jensen et.al "On technical issues in cloud computing", IEEE International Conference on cloud computing, CLOUD 2009, Bangalore, India, 21-25 September, 2009.
[5] Rabi Prasad Padhy et.al "Cloud Computing: Security Issues and Research Challenges "IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011
[6] S.S. Chopade et.al. "Securing Cloud Servers against Flooding Based DDOS Attacks" Communication Systems and Network Technologies (CSNT), 2013 International Conference on IEEE, 6-8 April 2013, Page(s):524 – 52 Print ISBN: 978-1-4673-5603-9, Gwalior.
[7] Joshi, Bansidhar et.al. "Securing cloud computing environment against DDoS attacks." Computer Communication and Informatics (ICCCI), 2012 International Conference on. IEEE, 10-12 Jan. 2016, Page(s): 1 – 5, Print ISBN: 978-1-4577-1580, Coimbatore.
[8] Shikha Singh et.al "Cloud Computing Attacks: A Discussion With Solutions " open journal of mobile computing and cloud computing Volume 1, Number 1, August 2014.
[9] J. Mirkovic and P. Reiher et.al. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms" ACM Sigcomm Computer Communications Review; Vol. 34, No. 2, Apr. 2004
[10] Chen R., Park J., and Marchany R., et.al. " A Divide and Conquer Strategy for Thwarting Distributed Denial of Service Attacks," Computer Journal of IEEE Transactions on Parallel and Distributed Systems, vol.18, no. 5, pp. 577-588,07
[11] Iqra Sattar et.al. "A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment" International Journal of Computer Applications (0975 – 8887) Volume 115 – No. 8, April 2015
[12] Qi Chen et.al. "CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment" Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference.
[13] Reddy, PallavaliRadha Krishna et.al "Analysis and Detection of DoS Attacks in Cloud Computing by Using QSE Algorithm." 2014 IEEE International Conference on High Performance Computing and Communications (HPCC), 2014 IEEE 6th International Symposium on Cyberspace Safety and Security (CSS) and 2014 IEEE 11th International Conference on Embedded Software and Systems (ICESS)
[14] Dawei Wang et.al. "Exploiting Artificial Immune System to Detect Unknown DoS Attack in Real Time" Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference vol.2, Hangzhou 10.1109/CCIS.2012.6664254
[15] MohdNazri Ismail et.al "Detecting Flooding based DoS Attack in Cloud Computing Environment using Covariance Matrix Approach", ICUIMC '13 Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication ,Article No. 36 ,ACM New York, NY,

USA ©2013 ,table of contents ISBN: 978-1-4503-1958-4

[16] Anitha, E., and S. Malliga.et.al "A packet marking approach to protect cloud environment against DDoS attacks." International Conference on. IEEE, 2013 Information Communication and Embedded Systems (ICICES), 21-22 Feb. 2013, Page(s):367 – 370, Print ISBN: 978-1-4673-5786-9 Chennai

[17] S.Mercyshalinie et.al. "Defense against DoS Attack: PSO Approach in Virtualization" 2014 Sixth International Conference on Advanced Computing (ICoAC), 17-19 Dec. 2014, Page(s):, 199 – 204, Chennai, ISSN: 2377-6927

[18] S. Ramgovind, M. M. Eloff, and E. Smith, "The management of security in Cloud computing," in Information Security for South Africa (ISSA), 2010, 2010, pp. 1–7.

