SURVEY OF CLOUD PROTECTOR USING IDS

1st Reena Research Scholar 2nd Parbhat Varma HOD Department of Computer Sc & Engg.. .

MIET Mohri Kurukshetra India

Abstract
Cloud computing poses a diversity of challenges in data mining operation arising out of the dynamic structure of data distribution as against the use of typical database scenarios in conventional architecture. Realization of maximum efficiency depends much on the initiation of accurate decision data mining. Cloud computing aims to provide convenient, on-demand, network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and ser- vices), which can be rapidly provisioned and released with minimal management effort or service provider interactions

***Index Terms*—CLOUD Computing,Attack,DDOS**

I. INTRODUCTION

Cloud Computing is the rapidly growing field of Information technology. Cloud Computing can be defined as an Internet based computing where Virtual shared servers provide software, infrastructure, platform devices and other resources. The main objective of Cloud Computing is that the customers use only what they want and pay only for what they use. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, customers are still reluctant to deploy their business in the cloud. Security issues in cloud computing has played a major role in slowing down its acceptance. In two surveys carried out by International Data Corporation (IDC) [1] in 2008 and 2009 respectively, security came top on the list. Although traditional threats are countered effectively but still some non-familiar risks have been introduced to the cloud. One such threat is Distributed Denial of Service (DDoS) attack. The DDoS attacks which took place in recent years have aroused the need for taking stern steps against it. A Denial of Service (DoS) attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system [6]. A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems [6]. On February 9, 2000 major DDoS attacks were waged against Yahoo.com, eBay, Amazon, E*Trade, ZDnet,, Buy.com, FBI and several other websites fell victim to DDoS attacks resulting in substantial damage and inconvenience[Garber 2000][7]. In 2004, series of DDoS attacks against variety of companies providing anti-spam services. These attacks caused companies to shut down their services. Hence it is very important to deter or otherwise minimize the damage caused by DDoS attacks.

II. DISTRUBTED DENAIL OF SERVICES (DDoS) ATTACK IN CLOUD

A Denial of Service (DoS) attack is an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system [6].In DoS attack legitimate users are unable to acces the data and services. In this attack attacker makes use of an individual system to attack another individual system.

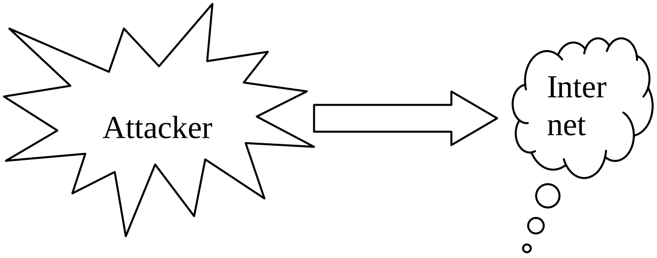
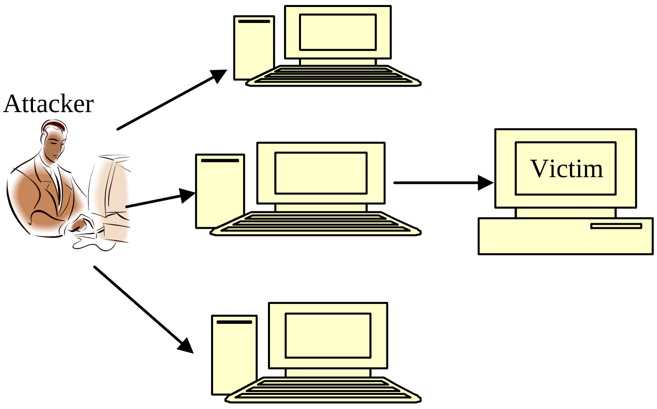


Figure-2.1 DoS Attack

DDoS is an advanced version of DoS. A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given target system or network that is launched indirectly through many compromised computing systems [6]. It also floods server with the large number of requests resulting in denial to the service requested by legitimate user. It is different from DoS attack as several machines are used in it for attack. As large number of systems are used in it thus it is difficult to trace the source of attack and difficult to defend the coordinated attack.



Symptoms of DDoS are:

- Speed of the system gets reduced and the programs run very slowly.
- Large numbers of requests from large number of users.
- Available resources become less in number.

The services under attack are those of the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims." The DDoS attack is mainly based on three functional units:
(1) *Master*: Master is the one who launches attack.
(2) *Slave:* Slave acts as a launch pad to the Master. Slave is actually a network. As it provides the platform for the attack to be launched it is also called co-ordinated attack.
(3) *Victim:* The server which is on the agenda of the Master to be attacked is the Victim. DDoS attack takes place in two stages.
DDoS attack takes place in two stages:
Stage 1: Intrusion Phase
During this phase the Master tries to compromise less important machine in order to get a support to flood the more important machines with requests.
Stage 2: DDoS tool installation phase
During this phase DDoS tools are installed in order to attack the victim or main server.
Thus, DDoS makes the service unavailable to the authorized user as in case of DoS but it is launched in the different way.
There are different types of attack packets used to perform DDoS attack. Basically attack packets are classified as follows[33]:

a) *TCP floods*: TCP is a connection oriented protocol. TCP flooding in DDoS attack works by exhausting the queue of TCP connection and therefore denying the request of legitimate user. To launch this kind of attack an attacker sends several SYN packets from forged IP addresses to the host machine. The host machine allocates memory queue to the SYN packets but attacker never acknowledges it. This will exhaust the memory of host machine and does not make host machine available to other legitimate user as it keeps on waiting for the ACK.
b) *ICMP floods:* A stream of ICMP packets is sent to host machine thus, slowing down the incoming and outgoing bandwidth. It may also result in overall shutdown of the system.
c) *UDP floods*: A UDP is connectionless protocol. Thus it is much easier than TCP flooding. It takes place by sending lots of UDP packets to host machine through forged IP addresses.

III. RELATED WORK

Saman Taghavi Zarger et.al in 2010 suggested a collaborative approach to facilitate IPSs for protection against DDoS attacks. For this an Autonomous System (AS) was taken. A collaborative IPS could distribute the sampling, detect and respond to the DDoS attacks. The proposed approach attains the coordination between various Autonomous System. It eliminates the redundant sampling. The assumptions made in design are: all routers within the AS can detect destination of flooding attacks, routing information and traffic matrix of network are available to the AS, for all approaches flow size is same. In Set up process all the paths, destination IPs and set o fall the routers are available in the traffic matrix. The objective of the approach is to reduce the gap between the loads of all the routers. A Linear Programming (LP) is formulated for assignment/optimization. The output of the LP formulation provides responsibility list of routers considering the objective of load balancing. The outcome of the measurements shows that the number of common Destination IPs does not have any adverse affect on the performance of the said approach. The drawbacks of this approach are: link flooding is not included in it; pre-computation of different clouds is not done.

Sanjay B. Ankali et.al in 2011 suggested a detection architecture for prevention from DDoS attack. The proposed system could detect DDoS attack on the basis of TCP connection and the behaviour of web user: how the user browses. Browsing behaviour described by three elements: http request rate, requested sequence and page viewing time. The architecture is divided into three parts: login, anomaly detection and prevention. SQL Server 2005 is used for storage of user's information related data. Front end is created by C#.NET. Anomaly Detection and behaviour detection is used for the detection of attack. The DDoS tools are used to spoof the original address of the user and thus save the secondary victim.
Chen Qi et.al in 2011 presented Confidence Based Filtering method named CBF. In this method the packets entering the cloud are distinguished whether they are attack packets or legitimate packets. To distinguish attack packets from the legitimate packets correlation patterns are used. The concept of correlation refers to the situation where some inferior characteristics take place at the same time when the packet flows. This means that the legitimate packet flows have unique correlation patterns. In this two terms are used: Confidence and CBF score. Confidence is the frequency of appearances of attributes in the packet flows. CBF score is the

weighted average of the confidence of the attribute value pairs. A discarding threshold is a threshold value set to judge the filtration. The legitimate packet will be that whose CBF score is above the discarding threshold. After distinguishing the packets the harmful packets are discarded and the request by the legitimate packets is satisfied. Then extensive simulations are conducted to evaluate the feasibility of the CBF method. The result shows that CBF have an acceptable filtering accuracy making it suitable for real time filtering in cloud environment. The drawback of this method is that although it is fast but it is costly method.

Pritesh Jain et.al in 2011 proposed an approach for Cloud bursting Brokerage and Aggregation (CBBA) for multi cloud environment through Class and Object. The proposed approach consists of four phases. In first phase the Cloud1 is opened for the implementation of the method on C++ files. In second phase an environment for cloud2 is opened where method is performed on Java files. In third phase cloud an environment for cloud 3 is opened where method is performed on C# files. In each phase object – oriented properties like class and object are calculated and according to those values aggregation and bursting are performed. In the last and the final phase sharing between clouds is performed under secure sharing mechanism. The sharing is done with security key so that only authorized person can access the cloud and share the resources between the clouds. The drawback of this approach is that it is just theoretical model.

Aderemi A. Atayero et.al in 2011 discussed the potentials of homomorphic encryption in security of cloud. Security has always been the alarming issue during the implementation of the cloud computing. According to International Data Corporation main issues cloud model are Security, availability and performance. Thus, a homomorphic encryption plays a good role in security issue. The homomorphic scheme allows the transformation of cipher texts of the messages to the cipher texts of the computation/ function of message without disclosing message.

IV INTRUSION DETECTION SYSTEM AND DDos SERVICES

Intrusion is a kind of Obstruction behavior, or an interruption, or interfering in someone's personal assets.
The general approaches to fight with DDoS include:

1 Extensive modification of the underlying network. But these modifications were costly to the users.

2 Swarm based logic to prevent DDoS attacks. In this logic a transparent transport layer is provided through which the common protocols such as HTTP, SMTP etc. can pass easily.IDS were introduced. IDS systems like SNORT were installed on virtual machines. The IDS system can also be installed on physical machines of users.

For handling issues of cloud IDS (Intrusion Detection system) are deployed. IDS is basically a part of computer security layer for detecting any kind of abnormal behavior on both i.e. over the network & over the host computer. For both Cloud providers and Cloud users IDS sensors in the Cloud is highly recommended. Cloud users need IDS to detect and prevent attack on their services. In order to protect Cloud environment from DoS and DDoS too IDS system need to be deployed in each cloud computing region.

S.No.	**Name of the attack**	**Function of the attack**	**Solution against the attack**
1.	Bandwidth Attack	Consumes target's resources	Multops, tree of nodes, detects the disproportional packets going and coming from the attacker
2.	ICMP (Ping) Flood	Bandwidth attack that uses ICMP packets	Screen OS, providing a Screening option which sets a threshold that once exceeded invokes ICMP flood attacks
3.	Ping of death	Sends multiple malformed or malicious pings to a computer	Add checks for each incoming IP fragment telling Whether the packet is invalid or valid.
4.	Amplification attack	Attacker makes a request that generates	Using high performance OS, load balancer,

		a larger response	limiting the connection rate.
5	DNS Flood	Attacks both infrastructure and DNS application	Radware carrier solution, allowing continuous DNS service even under the attack and mitigating the DNS attack.
6.	HTTP GET Flood	Attackers send a huge flood of requests to the server and consume its resources	NS FOCUS provides web application firewall, Intrusion prevention system, carrier-grade anti-DDOS system.
7.	Reflector Attack	Where third parties bounce the attack traffic from attacker to the target	DERM (Deterministic Edge Router Marking), helps in identifying, tracking and filtering the attack.
8.	Smurf Attack	Attackers use ICMP echo request packet to generate DOS attacks	Ingress filtering, configuring all the hosts and routers not to respond to ICMP requests and not to forward the packets directly to broadcast addresses.

V. CONCLUSION

This paper emphasized the usage of alternative options to incorporate intrusion detection and intrusion prevention techniques into Cloud. Cloud is a highly dispersed computing model which is still evolving, posing multiple challenges for data integration and distribution. Here, we tackled the problem of refined data heaping with a mining approach intended to collect and integrate relevant data

Refrences

[1] Saman Taghavi Zargar, James B. D. Joshi, "A Collaborative Approach to Facilitate Intrusion Detection and Response against DDoS Attacks". In the *Proceedings of the 6th international Conference on Collaborative Computing: Networking, Applications & worksharing , collaboratecom, Chicago, USA*. October 2010.

[2] Pritesh Jain, Dheeraj Rane, Shyam Patidar, "A survey and Analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Aggregation in Renal Environment", In *World Congress on Information and Communication Technologies*. pp. 456-461, IEEE, 2011.

[3] Sanjay B Ankali, Dr. D V Ashoka, "Detection Architecture of Application Layer DDoS Attack for Internet". In International Journal of Advanced Networking and Applications, Vol-o3, Issue: 01, pp. 984-990, 2011.

[4] Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu, "CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment", In *Ninth International Conference on Dependable, Autonomic and Secure Computing*, pp.-427-434, IEEE, Jan 2011

[5] Aderemi A. Atayero, Oluwaseyi Feyisetan,"Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption", In *Journal of Emerging Trends in Computing and Information Sciences*, Vol-2, No.10, pp.546-552, October 2011

[6] W. Yassin, N.I. Udzir, Z. Muda, A. Abdullah, M.t. Abdullaha, "Cloud-Based Intrusion Detection Service Framework". In the *Proceedings of the International*

Conference on Cyber Security, pp. 213-218, IEEE, June 2012
[7] Abhishek Jain, Ashwani Kumar Singh, "Distributed Denial of Service (DDOS) Attacks – Classification And Implications". In *Journal of Information and Operations Management*, ISSN: 0976-7754 & E-ISSN: 0976-7762, Vol. 3, Issue 1, pp 136-140, 2012
[8] http://www.symantec.com/connect/articles/justifying-expense-ids-part-one-overview-rois-ids