AN EFFICENT DETECTION AND PREVENTION OF DDOS ATTACKS IN CLOUD ENVIRONMENT

[1]R.T.Anitha,[2] Dr B. Ananthi

[1]Research Scholar, Department of Computer Science, Vellalae College for Women, Erode, Tamil Nadu, India.

[2]Associate Professor & Head, Dept. of Computer Science(UG & PG), Vellalar College for Women,

Tamil Nadu, India.

ABSTRACT

Distributed Denial of Service (DDoS) attacks in cloud computing environments are increasing due to the essential characteristics of cloud computing. DDoS attacks are cyber-attack where the network resources are unavailable to its users by temporarily. Distributed denial-of-service (DDoS) attacks are major security problem, the mitigation of which is very hard especially when it comes to highly distributed botnet-based attacks. Even if, the early detection of these attacks, are challenging, it is necessary to protect end-users as well as the expensive network infrastructure resources.In this paper, Address the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms of FireCol. FireCol comprises of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. The detect of DDoS attack can be performed by FireCol algorithm along with the threshold value. Load balancing is one of the main challenges, important technique, critical issue and play an important role which is required to distribute workload or task equally across the servers and with the help of PSO (Particle Swarm Optimization) algorithm data will be split into different packets and then stored in the server. The Paper focused FireCol algorithm that detect and prevent the DDoS attacks. Experimental result are presented to test the security of FireCol algorithm.

KEYWORDS: DDoS attack, Cloud Computing, Firecol, and PSO.

1 INTRODUCTION

Internet is the most popular technology and its usage is rising over a period. In industry, organizations, offices, business, government sector, and many other sectors are using internet while running their business. Cloud computing is internet based computing where virtual shared servers provide software, infrastructure, platform, devices and other resources and hosting to customers on a pay-as-use basis.

Objective of the problem

DDoS is a Distributed Denial of Service. DDoS is a type of DoS attack, DoS means a single system is affected by a Trojan is a Denial of Service, DDoS where multiple compromised systems, which are infected with a Trojan. In a DDoS attack, the incoming traffic flooding the victim originated from many different sources potentially hundreds of thousands. This effectively makes it impossible to stop the attack simply by blocking a single IP address.

Types of DoS/DDoS attacks

There are several types of DDoS attacks as follows

Flood attack

DDoS attack is also known as ping flood. It is based on an attacker simply send the victim large number of ping packets, usually and using the "ping" command, so the victim can handles more traffic.

Ping of death attack

The ping of death attacks sends oversized Internet Control Message Protocol (ICMP) packets. It is one of the core protocols of the IP. The maximum packet size allowed is 65,536octets. Some system upon receiving the oversize packets will crash or freeze resulting in DDoS.

SYN attack

It is also termed as TCP SYN Flood. Transmission Control Protocol (TCP), handshaking of network connection is done with SYN and ACK message. An attacker initiates a TCP connection to the server with an SYN (using a legitimate or spoofed source address). The server replies with an SYN-ACK. The client then does not send back an ACK, because the server to allocate memory for the pending connection and wait.

Teardrop attack

The teardrop attack is used to fragmented packets are forged to overlap each other, when the received host tries to reassemble them. IP's packet fragmented is used to send corrupted packet to confuse the victim Figure 1 DDoS attack [1].

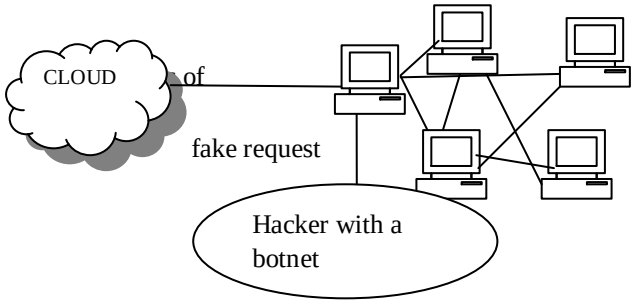

Figure 1 DDoS attacks

Classification of DoS attacks

Protocol attacks

The data are sending over the network. These attack specific feature implementation bug of some protocol installed at the victim system to consume excess amount of its resource.

Network Device Level

DoS attacks in the network Device Level include attacks that taking an advantage of bugs or weakness in software, or by trying to exhaust the hardware resource of network devices. Example: Network device could be connected to the router via telnet enters the long password it will crash.

OS Level

OS Level attacks take a ways of operating system implemented protocols. Example: Ping of Death attack.

Application Based Attacks

In network application that are running on the target host or by using such application to drain the resource of their victim. It is also possible that the attacker may have found points of high algorithm complexity and exploits them in order to consume all available resources on the remote host.

Data flooding attacks

Any website is loading it's take a certain time. Loading means complete webpage appearing on the screen, the system is awaiting user's input. This loading consumer some amount of memory. Every site is given with a particular amount of bandwidth for its hosting Figure 2 Classification of DDoS.

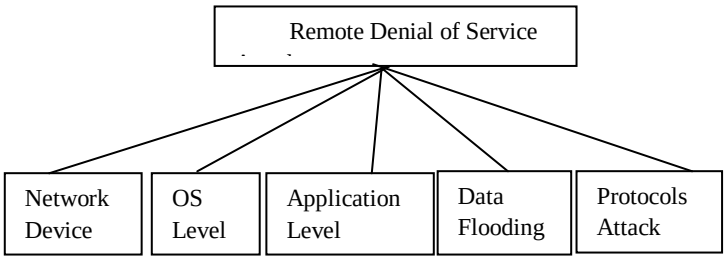

Figure 2 Classification of DDoS

Load balancing

Large qualities of data are generated and exchanged over the network which needs more and more computing resources. Organizations, already using cloud-based services in one or the others form. It is brings us to the concept of load balancing in cloud.

Cloud load balancing is the process of distributing workloads and computing resources across one or more servers. This kind of distribution is maximum throughput in minimum response time. Workload is segregated among two or more servers, hard drives, network interfaces or other computing resources, enabling better resource utilization and system response time.

The common objectives of using load balancers are:

- To maintain system firmness.
- To improve system performance.
- To protect against system failures.

Advantage of cloud load balancing

High performing applications

Enterprises can make their client applications work faster and deliver better performances, that too at potentially lower costs.

Increased scalability

Cloud balancing is used to scalability and agility to maintain website traffic. By using efficient load balancers, user can easily match up the increased user traffic and distribute it among various servers or network devices.

Ability to handle sudden traffic spikes

Normally running university site can completely go down during result declaration. It is because too many requests can arrive at the same time. If they are using cloud load balancers, they do not need to worry about such traffic surges. It can be wisely distributed among different servers for generating maximum result in less response time.

2 RELATED WORK

TARIK TALEB et al., [2014][2] The article discusses the challenges these trends present to mobile network operators. It also demonstrates the possibility of extending cloud computing beyond data centers to the mobileend user, providing end-to-end mobile connectivity as a cloud service. The article introduces a technologies and methods for on-demand provision of a decentralized and elastic mobile network as a cloud service over a distributed network of cloud computing data centers. Mobile operators are in need of means to cope with the ever increasing mobile data traffic, introducing minimal additional capital expenditures on existing infrastructures, principally due to the

modest average revenue per user. Network virtualization and cloud computing techniques, along with the principles of the latter in terms of service elasticity, on-demand, and pay per- use, could be important enablers for various mobile network enhancements and cost reduction. This article introduces the concept of the carrier cloud, its high level architecture, and the mechanisms to achieve it. To achieve the carrier cloud, there is also a need for network function virtualization whereby the software components of mobile core network nodes are decoupled from the hardware.

Iqra Sattar et al., [2015][3] Proposed DDoS attack prevention and detection. DDoS attack is occurs when huge amount of data or packets are sent to a server from various computer. So it is a one of major causes of DDoS attack. Here apply several techniques to avoid the DDoS attacks. TTL algorithm is monitored continuously over the cloud network using three parameters are a)SYN flag b) TTL c) source IP. Another algorithm is use that is CBF (Confidence Based Filtering) packet filtering method is used to reduce the storage needs and increase the processing speed on the server side. Finally use various techniques detecting and preventing the DDoS attack in cloud computing system. To improve availability of resources, it is essential to provide a mechanism to prevent DDoS attacks.

George Pallis et al., [2010][4] says that cloud computing raises issues in the architecture, design, and implementation of existing networks and data centers. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (for example; networks, servers, storage, applications, and services) that can be quickly provisioned and released with minimal management effort or service provider interaction. Cloud computing grew out of our never-ending hunger for ever-faster and ever-cheaper computation. The key driving forces behind it are the promise of broadband and wireless networking ubiquity, lower storage and mobile device costs, and progressive improvements in Internet computing software and mobile computing. The perceived advantages for cloud-service clients include the ability to improve use by adding more capacity at peak demand, reducing costs, experimenting with new services, and removing unneeded capacity.

F. Richard Yu et al., [2015][5] proposed jointly consider cloud radio access networks (C-RAN) and mobile cloud computing (MCC) in a holistic framework. Propose an optimal policy for the stochastic optimization problem, which has the merit of low computation cost. Offline and online algorithms are developed based on the optimal policy. Use simulation results; show that, with the emergence of MCC and C-RAN technologies. That design and operation of future mobile wireless networks can be significantly affected by cloud computing and the proposed scheme is capable of achieving substantial performance gains over existing schemes. Unlike the existing cellular networks, where computing resources for baseband processing are located at each cell site, in C-RAN, the computing resources are located in a central wireless network cloud with powerful computing platforms.

Ying-Dar Lin and Dan Pitt et al., [2014][6] Discuss about the emerging second wave, software-defined networking (SDN), takes network centralization and virtualization, and especially network control in the cloud. After emerging in datacenters, SDN deployment has grown up into the networking-as-a-service (NaaS) model cloud service providers now offer to enterprise and

residential subscribers. By centralizing control-plane software (the network that carries the signaling traffic responsible for routing is a part of the software controlling) to the controller and its applications, and controlling the device data plane (the actual data-packet movement) remotely, devices can become simpler.Thus, SDN significantly reduces the administrators required and as a result reduces expenses, both capital and operational.The data plane is highly programmable from the remote control plane at controllers and applications because SDN also enable fast service orchestration. In general, SDN takes networking into the computing domain and will increasingly adopt the standardization practices common for computing and software.

3 DDOS ARCHITECTURE

Archiecture diagram is a graphical representation it is used to detect the attak in cloud. The system includes two sub-systems: the detection sub-system and prevention sub-system, as shown in below Figure3.

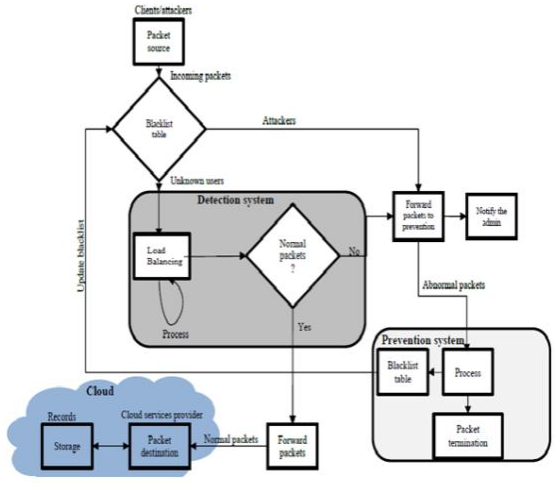

Figure 3 Architecture of DDoS system

Detection phase

During the detection phase, the detection sub-system collects the incoming packets within a time frame, for example 60 seconds. The collected packets are subjected to a blacklist check to test whether their sources are blacklisted as attackers of the cloud system. If the packet source is listed in the attacker blacklist, the detection system will send the packets directly to the prevention sub-system without further processing. If the packet source is not blacklisted, the incoming packet will be passed to the classifier to decide whether the packets are normal (originating from a client) or abnormal (originating from an attacker). A packet is considered to be an attacking one if the source requests connections to the same destination more frequently than an assumed threshold. The threshold can be manually adjusted by the system administrator to cater for the varying requirements of a particular network. If a packet is considered to be normal, the detection system will send it to its destination (the cloud service provider). Otherwise, the detection sub-system will send the packet to the prevention sub-system.

Prevention phase

When the packets reach the prevention system, they are considered to be attacking packets by the detection sub-system. The prevention sub-system first alerts the system administrator of the attacks. Then, the prevention sub-system will add the attacking source address to the attacker blacklist used by the detection sub-system, if it is not already on the list. Finally, the attacking packet will be dropped. The overall architecture of the DDoS system is shown in Figure3.

METHODOLOGY

a) Firecol Algorithm

If each selected r_i, the collaboration manager computed the corresponding packet rate using rule frequencies and the overall bandwidth (bw_m) consumed during the last detection window. If the rate is higher than capacity cap_i, an alert is raised.

1. If $b_i \wedge$(IPS_id ≠ null) then
2. If IPS_id == my ID then
3. B_i = false;
4. Return
5. Else
6. $Rate_i \leftarrow rate_i + F_i$
7. If $rate_i > cap_i$ then
8. B_i = false;
9. Raise DDoS alert;
10. Return
11. Else
12. nextIPSCheckrules(IPS_id,I,rate,cap_i)
13. endif
14. endif
15. else
16. b_i = true;
17. next IPS.checkRule(myID,I,0,cap_i)
18. endif

Otherwise, the computed rate is sent to the next IPS on the ring. When an IPS received a request to calculate the aggregate packet rate for a given rule, it first checks if it was the initiator. In the case, it deduces that the request has already made the round of the ring, and hence there is no potential attack. Otherwise, it calculates the new rate by adding in its own rate and checking if the maximum capacity is reached, in which case an alert is raised. Otherwise, the investigation is delegated to the next horizontal IPS on the ring. This retail algorithm show below It is initially called with an empty IPS_{id}. The first IPS fills and sets the boolean b_i to true. b_i is reset after the computation finishes. i.e., When the request has made the round of the ring or when the alert is triggered. With simple adjustments, ring traversal overhead can further be reduced if several suspect rules are investigated in one pass.

Rate computation can be performed based on the number of packets per second or byte per second. The first method is more suitable for detection flooding DDoS attacks having a small packet pattern, such as SYN floods. Bytes-based method is better for detection flooding attacks with large packet payloads. Firecol customers can subscribe to either or both protection types.

b) PSO (Particle Swarm Optimization) Algorithm

PSO is influenced by social behavior of animal like flock of birds finding food source. A Particle is analogue to bird flying through problem space. Each Particle contains velocity and solution. The performance of particle is measured by fitness value which is problem specific.

In this algorithm particles are initialized randomly. Each Particle contains fitness value which is calculated by fitness function. Each Particle known its best position p^i_k and best position among entire group of particles p^g_k. In each generation velocity and position of each particle is updated using following equation.

$$V^i_{k+1} = v^i_k + c_1 r_1 (p^i_k - x^i_k) + c_2 r_2 (p^g_k - x^i_k)$$

$$X^i_{k+1} = x^i_k + v^i_{k+1}$$

V^i_k is the particle velocity, x^i_k is the current particle. P^i_k and p^g_k are defined as stated before. R_1 and r_2 is a random number between (0,1). $C_{1,}c_2$ are learning factors. Usually C1=C2=2.

For each particle
Initialize particle
END
DO
For each particle
Calculate fitness value
If the fitness value is better than the fitness
Value(p^i_k) in history
Set current value as new p^i_k
End
Choose the particle with the best fitness value of all
the particle as the p^g_k
For each particle
Calculate particle velocity according equation(a)
Update particle position according equation(b)
End

4 RESULTS AND DISCUSSION

FireCol method is applied for 3 way intrusion detection system. The detection accuracy level for existing and proposed algorithms are shown in Figure 4. The core of FireCol is composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. In existing methods, detection accuracy is less to find the intrusion detection. So the proposed system FireCol algorithm is little higher than the existing.

Sensitivity also called probability of detection; it measures the proportion of positives that are correctly identified such as error/intrusion. Degree of awareness and responsiveness to internal or external changes made by intruers.

PORT SCANNING

A port scanner is an application designed to probe a server are host for open ports. Port Scanner used by administrator to verify security polices for their networks and by attackers to indentify network services running on a host and exploit vulnerabilities.

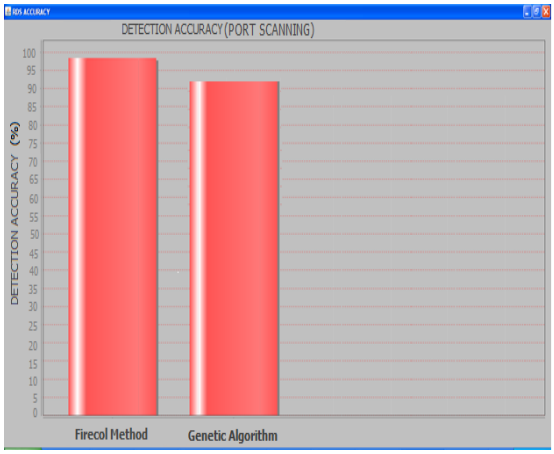

Figure 4 Port Scanning Graph

ALGORITHM	ACCURACY	SENSITIVITY
Genetic Method	93%	91%
Firecol Method	98%	97.5%

Table: 1 Port Scanning

Table 1 shows Port Scanning process using FireCol method. This table shows the detection accuracy and sensitivity.

SYN FLOODING

A SYN Flood is a form of denial-of-services attacker in which an attacker sends a succession of SYN request to a target system in an attempt to consume enough server resource to make the system unresponsive to legitimate traffic.

Figure 5 SYN Flooding

ALGORITHM	ACCURACY	SENSITIVITY
Genetic Algorithm	94%	90%
FireCol Method	98%	97%

Table: 2 SYN Flooding

A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic. Table 2 shows how to find SYN Flooding attack more efficiently than existing method. FireCol method finds 98% accurate result in SYN Flooding attack.

PING OF DEATH

Ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol.

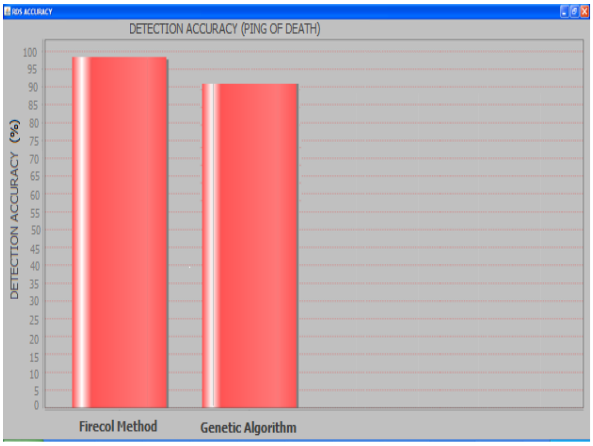

Figure 6 Ping of Death

ALGORITHM	ACCURACY	SENSITIVITY
Genetic Algorithm	91%	85%
FireCol Method	97%	96%

Table: 3 Ping of Death.

The Ping of death attacker intrudes through the internet. Proposed method finds the attacker more efficiently than existing method.

5 CONCLUSION

The use of cloud computing in many sectors is becoming widespread, as this helps to improve the system in many aspects. However, these cloud works are vulnerable to certain types of attacks, such as DDoS TCP flood attacks, this approach to determine the classified incoming packets of behavior in source within a time frame, in order to discover whether the sources are associated with a genuine client or an attacker. In this thesis conclude that, the three processes like Ping of Death, Port scanning and SYN flooding are compared with existing accuracy is better than proposed accuracy. The results are shown by using classification in DDoS attacks to identify the attacks accurately so proposed approach can

efficiently improve the security of data, reduce bandwidth consumption and mitigate the exhaustion of resources.

In the future, aim to extend DDoS to overcome the problem of DDoS using spoofed IP addresses as well as to improve the proposed work to identify the attackers even when they satisfy the threshold value. We strongly believe that combining source address authentication, capability mechanisms, and filtering mechanisms could be the most effective and efficient way to address the DDoS flooding attacks in a distributed cooperative/collaborative DDoS defense mechanism. The incorporation of the results of the attackers incentives analysis into future defense strategies i.e., this may lead to different strategies based on the attacker's motivations.The employment of the cross layer traffic analysis and defense mechanisms i.e., looking at the information at multiple protocol layers simultaneously to detect and respond to the DDoS flooding attacks. The development of strict cyber-crime laws and multi-national enforcement mechanisms along with refined cyber-insurance policies that require implementation of DDoS detection and prevention mechanisms.

REFERENCE

1) Kamlesh Bajaj. "Cyber Security." Wiley Indian Private Ltd., 2011, Delhi.
2) T. Taleb, "Toward carrier cloud: Potential,challenges, and solutions," IEEE Wireless Comm., vol. 21, no. 3, pp. 80–91, June 2014.
3) Iqra Sattar "A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment," International Journal of computer Applications, Vol.15, No.8, April 2015.
4) G. Pallis, "Cloud computing: The new frontier of internet computing," IEEE Internet Computing, vol. 14, no. 5, pp. 70–73, Sept. 2010.
5) Y. Cai, F.R. Yu and S.Bu, "Dynamic operations of Cloud radio access networks(C- RAN) for mobile cloud computing system," IEEE Trans. Veh. Tech., 2015, doi:10.1109/TVT.2015.2411739, online.
6) M. D. Yosr Jarraya, Taous Madi, "A survey and a layered taxonomy of software-defined networking," IEEE Commun. Surveys & Tutorials, vol. 16, no. 4, pp. 1955–1980, Fourth Quarter 2014.
7) Z. Yin, F. R. Yu, S. Bu, and Z. Han,"Joint cloud and wireless networks operations in mobile cloud computing environments with telecom operator cloud," IEEE Trans. Wireless Commun., vol. 14, no. 7, pp. 4020–4033, July 2015.
8) Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 2, pp. 843–859, SecondQuarter 2013.
9) S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEECommun. surveys & Tutorials, vol. 15, no. 4, pp. 2046–2069, Fourth Quarter 2013.