SURVEY ON MITIGATION TECHNIQUES OF ECONOMICAL DENIAL OF SUSTAINABILITY ATTACK IN CLOUD COMPUTING

Upasana Leela[1], Prof. Zishan Noorani[2]

[1]M.E. Student, Dept. of Computer Engineering, L.D.College of Engineering, Gujarat, Ahmedabad
[2]Assistant Prof. Dept. of Computer Engineering, L.D.College of Engineering, Gujarat, Ahmedabad

---

Abstract - *The promise of pay-as-you-go and scalable model of cloud computing has attracted a large number of medium and small enterprise to adopt E-commerce model of conducting on-line businesses. While E-commerce applications on cloud expand businesses by making them more widely acceptable, they also make these application susceptible to economic denial of sustainability attacks a form of application layer Distributed Denial of Service attack that drive up the cost of cloud computing by using up application resources. Economical Denial of Service attack intention is to consume all the resources (like memory, bandwidth and CPU etc.) of the web server thus making it unavailable to its legitimate users.*

Key Words: Cloud computing, DDoS, EDoS, EDoS-Shield, EDoS-ADS, EDoS-Eye

1. INTRODUCTION

Cloud computing is a strong contender to traditional IT implementations as it offers low-cost and "pay-as-you-go" based access to computing capabilities and services on demand providing ease users[1]. The cloud resources can be provisioned and frees with minimal cloud provider interaction by using an auto scaling feature. The auto scaling feature is activated by monitoring parameters such as CPU utilization, memory usage, response time and bandwidth.

1.1 INTRODUCTION TO DOS ATTACK

1. DoS and DDoSAttack

DoS attackers target the server, which is providing a service to its users, behaving like legitimate user, DoS attackers try to find active servers in such a way that service becomes unavailable due to large number of request pending and overflowing the service queue. A distributed DoS where attackers are group of machines targeting a particular service[1]

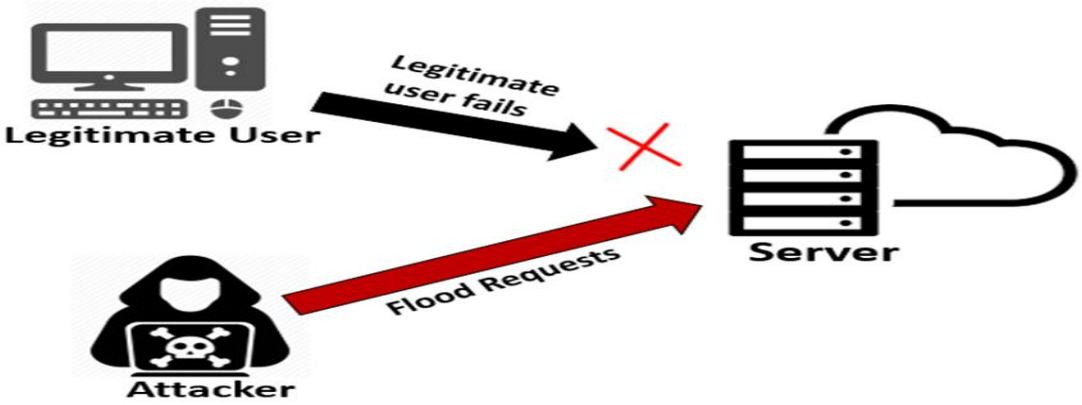

Fig -1: DoS Attack[1]

DDoS attacks have recently been very successful on cloud computing, where the attackers exploit the "pay-as-you-go" model. The three important features are reason behind the success trends of cloud computing. The same features are proven to be helpful to DDoS attackers in getting success in attacks. Those features are:Auto-scaling,Pay-as-you-go account and multi-tenancy[1].

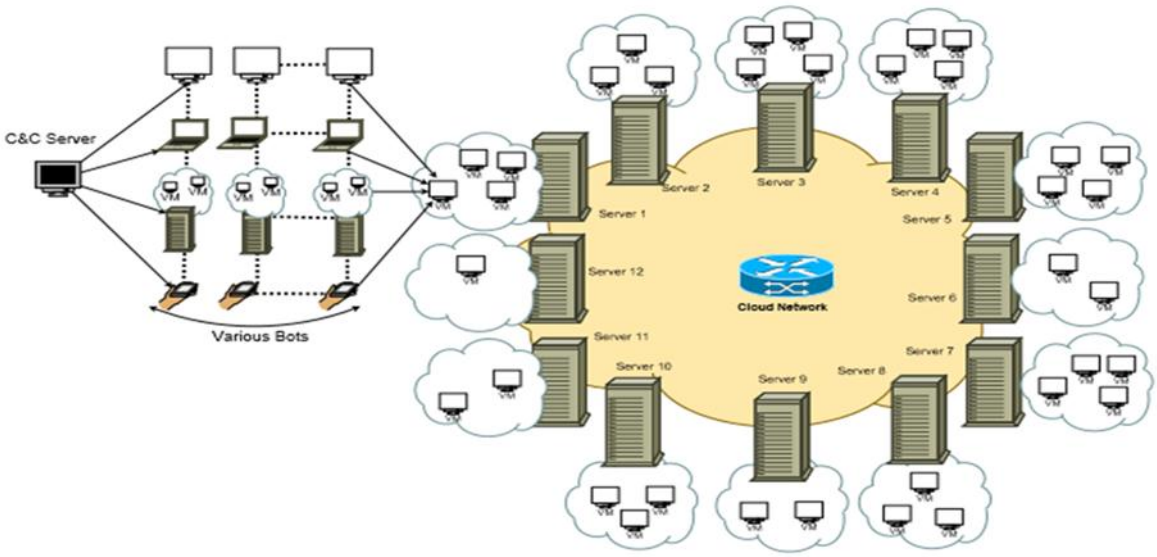

Fig -2: DDoS Attack[1]

2. EDoS Attack

The introduction of resource rich cloud computing platforms, where adopters are charged based on the usage of cloud's resources known as "pay-as-you-use" has transformed the Distributed Denial of Service(DDoS) attack problem in the cloud to financial one. This new type of attack targets the cloud adopter's economic resources and referred to Economical Denial of Sustainability(EDoS) attack [2].

A well-known tactic taken by EDoS attacks is to remotely control zombies to smoothly flood targeted cloud service by undesired requests. As a result of these requests and because of cloud elasticity feature, the service usage will be scaled up to satisfy the on-demand requests. And because of "pay-as-you-go", a cloud adopter's bill will be charged for those request leading to service withdrawal or bankruptcy.

2. Related Work

1.1 EDoS shield[2]

EDoS shield[] is a mechanism for mitigating EDoS in cloud computing. Main components of the architecture are: virtual firewall(VF) and verifier nodes(v-nodes).The virtual firewalls are used as filtering mechanism, Filtering is done based on IP address of source nodes as black list or white list. These lists are updated based on verification process.

The v-nodes has capability to verify legitimate users using graphical turing tests. V-node will update the virtual firewall list based on result of verification process. Black listed source addresses will be blocked for further requests. The whitelisted IP addresses will be served destined service.

Analysis results:

With the proposed mitigation technique, the response time corresponding to legitimate clients is approximately constant and low. The computing power utilization is not affected due to the attack rate since the attack requests will not reach the protected cloud service. The cost is constant since the rate of the legitimate requests is fixed

Advantages: This approach does not suffer from the problem of location-hiding as it is not required in our approach to hide the location of the protected cloud service.

Drawbacks:

Decreasing the response time, Not protecting the Scalability and no Strong Authentication

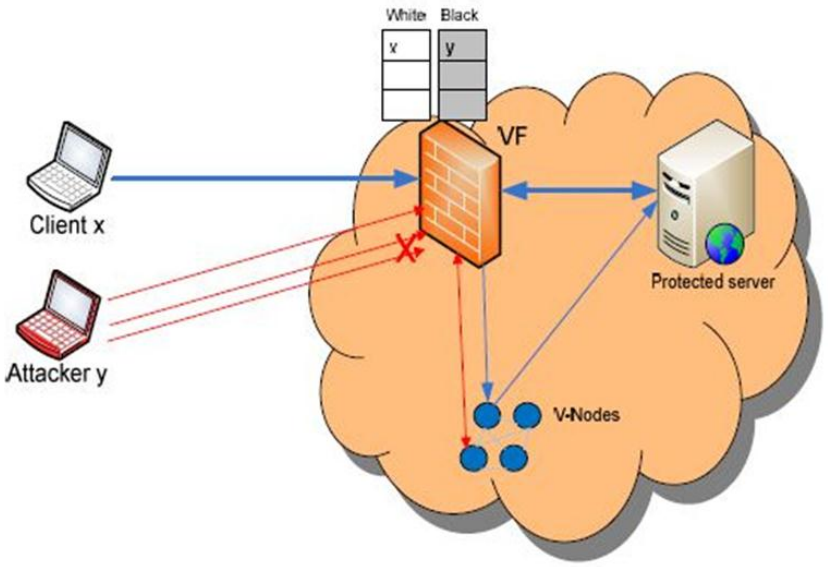

Fig -2: EDoS-Shield framework

1.2 Enhanced EDoS shield[3]

Architecture is same as of EDoS-shield with components as Virtual Firewall and V-nodes but it also looks into TTL values and counter of unmatched TTL for IP spoofing. Timestamp field in the black list is used to record start time of attack, which is time at which source IP address is put into blacklist every time TTL of requesting node is matched with VF table. Instead of dropping because of non-matching TTL, verification process will be done.

Four cases need to be considered in this as:

1. New request:

V-node performs verification using Graphical Turing Test(GTT), If pass then add IP to whitelist else blacklist with TTL, timestamp and unmateched counter will be incremented.

2. IP address in White list:

V-node performs verification phase, if it passes then just TTL will be updated and if it fails, Unmatched TTL counter will be incremented and IP will be added to blacklist with TTL and timestamp.

Case 3: IP address in Black list:

Packet dropped when TTL values matches or unmatched TTL counter exceeds threshold during attack lifetime. Otherwise V-node will perform verification process, if pass then add into whitelist and proceed. If fails, the verification then packet is dropped and entry in blacklist is updated.

Case 4: Both in whitelist and Blacklist:

Packet will be dropped when TTL matches in blacklist otherwise verification will be done.

Drawbacks:

Maximum allowable changes made to TTL value in proposed algorithm, it has been set to value of 5.

Effectively detect attack from individual but not able to prevent pattern attack

1.3 Enhanced DDoS-MS[4]

Enhanced DDoS-MS consists of Firewall, Client Puzzle Server(CSP), Intrusion Prevention System(IPS) and Reverse Proxy server(RP).

Verifier node is used to verifier using GTT. Firewall holds four lists: Black list, White list, Suspicious list and Malicious list. IPS is used to check content of the packet. RP server is used to hide location of protected server and to load balancing. Client puzzle server is used to verify when suspicious user is found.

Scenarios will be like: If it's the first requested packet, it will send GTT for verification. If user is in whitelist, it will be checked for TTL. If user is in black list TTL and start time is updated. The packet will pass through IPS, it will check for malware components. If malware components will be found, It will drop the packet and IP will be added to Malicious list. Then packet will pass through RP server, it will check for no. of packets, If found malicious packet then it will drop the packet and will add the IP to suspicious list. If IP is in suspicious list, it will be verified by V-node using GTT, If GTT is passed then will be further tested through puzzle server using crypto puzzle, if it fails the will be added to malicious list otherwise proceed further. If IP is in Malicious list packet will dropped.

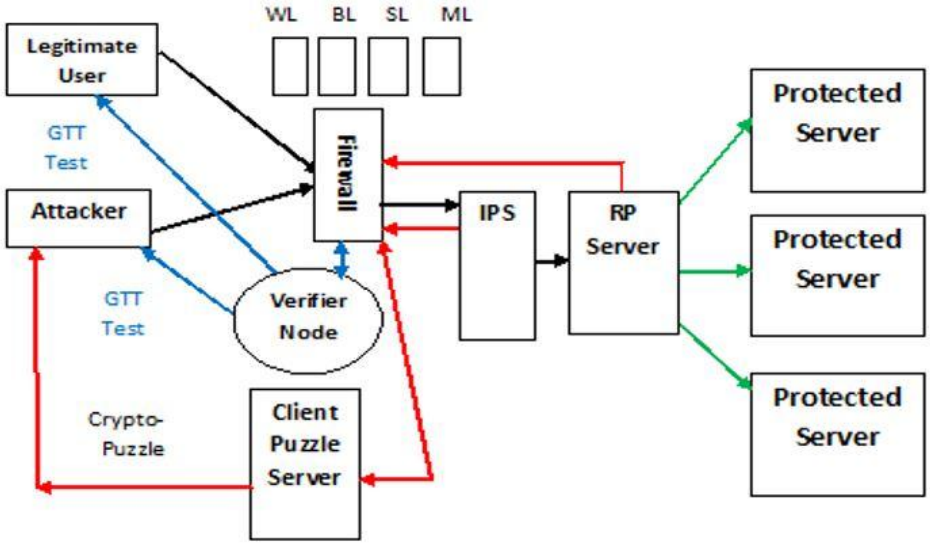

Fig -2: DDoS-MS framework[4]

Drawbacks:

The legitimate clients successfully pass the Turing test and the other checks but they flood the protected server by a large number of requests from a large number of legitimate sources.

1.4 EDoS Eye[5]

Edge router is gateway of both attack and legitimate traffic flows. The aggregate flow then distributes evenly through load balancer. Virtual firewall instances receive the distributed incoming flows. After filtering in virtual firewall instances, a portion of traffic reached at target VMs. Honeypot is incorporated, it is probing device to analyze traffic even it can capture new signatures of attack. Game Based Decision Module(GBDM) is integrated with virtual firewall, it generates optimal threshold values K1 and K2 to rate limit the incoming traffic.

Drawbacks:

Assumes Single attacker attack and as one flow from VMs/Bots.

Nothing is saved for checking IP next time, whole process is done as new.

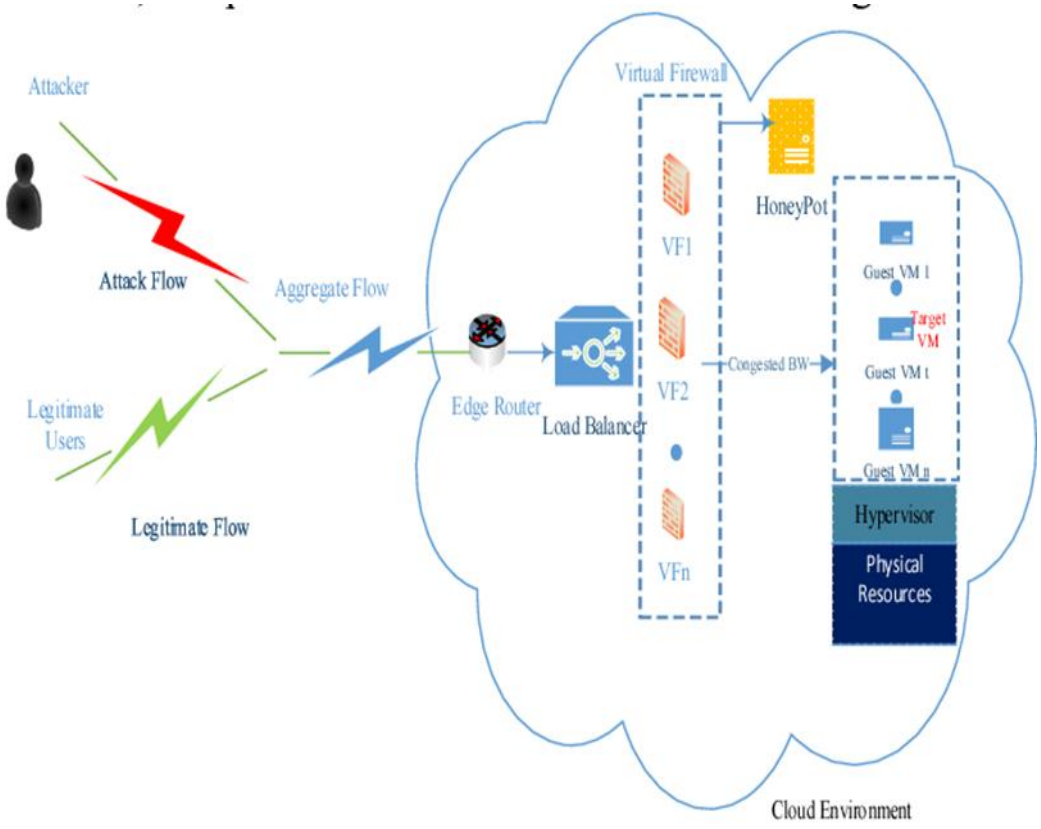

Fig -5: EDoS-Eye framework [5]

Flow is presented as bellow:

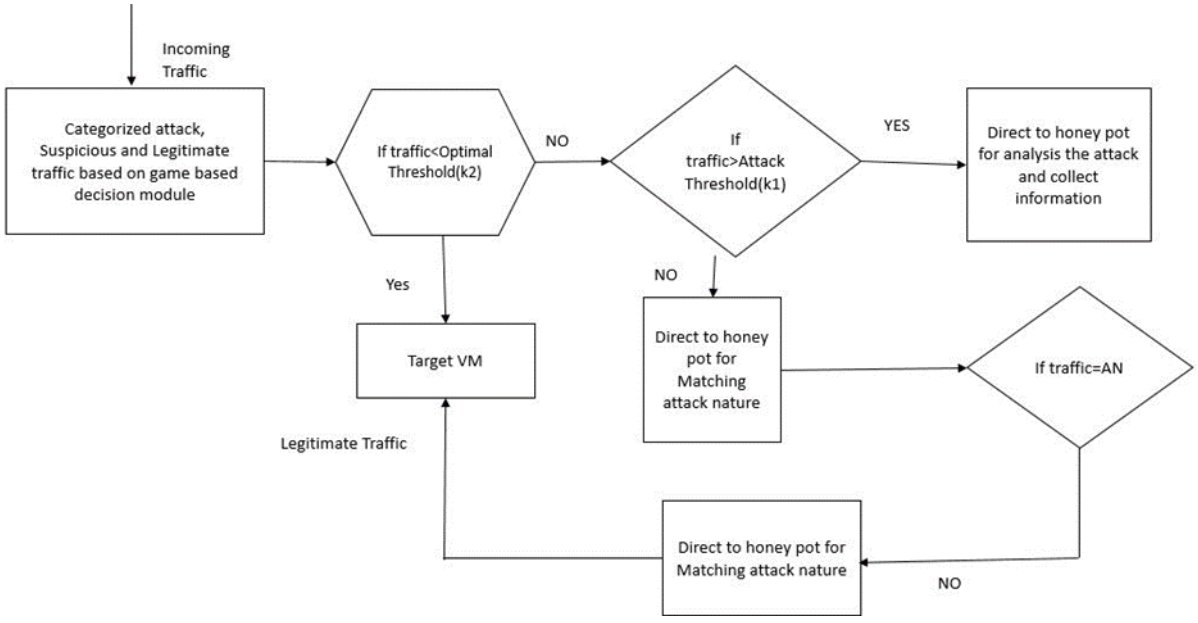

Fig -5: EDoS-Eye workflow[5]

1.5 EDoS-ADS[6]

It consists of Load balancer, Database and Defense shell. Works in four modes: Normal, Suspicion, Flash overcrowd and Attack mode. Defense shell work in different mode for different mode as suspicion shell and attack shell for suspicion mode and attack mode.

When Scaling-up upper threshold does not exceed limit, it works in suspicion normal mode. When it exceeds it, works in suspicion mode. Trust Factor (TF) value of user is set by suspicion shell. It is between o to 1 and by default o.5.If GTT failed then TF value is decremented and marked as suspicious user.

Virtual IP is provided by Defense shell. Upon receiving request, DS updates values of last seen and client request time. If time difference is more than one second Current request per second(CRPS) is set to 1 otherwise CRPS in incremented. Total Request Counter(TRC) is also maintained.

Suspicion shell:

If Current request per second(CRPS)<=Maximum request per second, then send URL redirection.

If CRPS>MRPS

Send URL redirection if client has good trust factor. It sends GTT to new clients if TF is low or average.

Suspicion shell counts no. of failed requests. It is triggered for upper threshold timer period. If timer does not expire and system utilization is decremented, then mode will be changed to Normal mode otherwise either in flash crowd or attack more. If MRC/TRC is 8% then new VM instances will be created and provisioning timer starts in flash overcrowd mode or in attack mode.

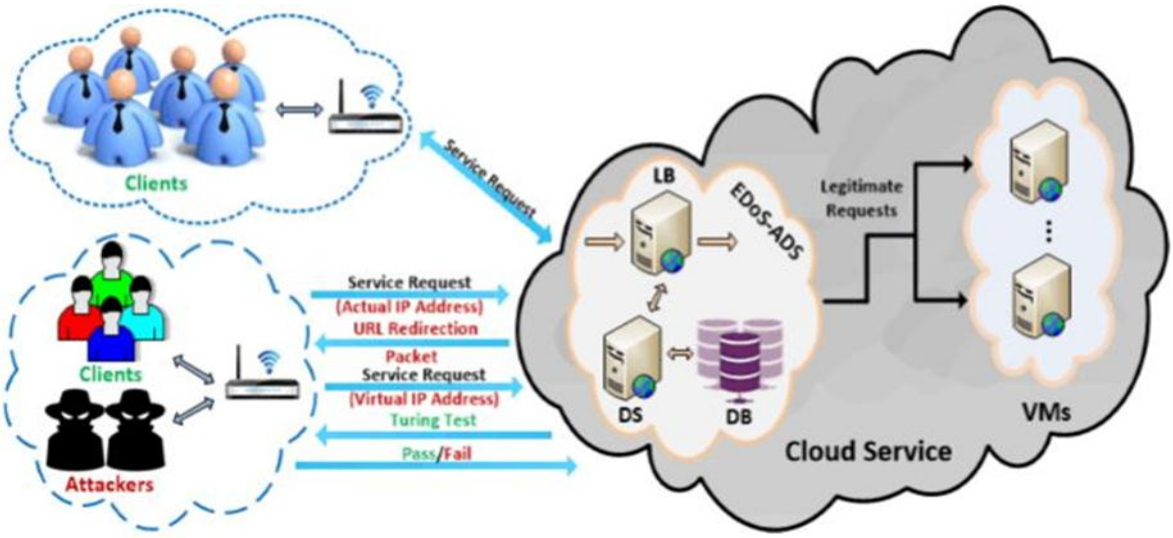

Fig -6: EDoS-ADS framework[5]

Attack Shell:

Sends URL redirect packet.

If client uses virtual IP address, If it does not exceed allowable RPS, it will be served otherwise GTT will be send.

If it fails to use virtual IP it will drop the packet.

Drawbacks:

URL direction to legitimate users also which may lead to flooding at that point.

User is not checked for until CPU utilization exceeds.

3. CONCLUSION

In this paper, we have conducted survey of different EDoS mitigation techniques. It shows basically how the technique works and what are the advantage and drawbacks are there in those techniques so that we can enhance the work in future. EDoS ADS is better than the EDoS-Shield in terms of performance metrics. EDoS-ADS seems better but it increases end-to-end delay.

REFERENCES

[1] Gaurav Somania,b, Manoj Singh Gaurb, Dheeraj Sanghic, Mauro Contid, Rajkumar Buyyae," DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions", Elsevier, August 29,2017

[2] Fahd Al-Haidari, Mohammed H. Sqalli, Khaled salah," Enhanced EDoS-Shield for Mitigating EDoS Attacks Originating from Spoofed IP Addresses", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012

[3] Mohammed H. Sqalli, Fahd Al-Haidari, khalad salah"EDoS-Shield - A Two-Steps Mitigation Technique against EDoS Attacks in Cloud Computing" ,in Fourth IEEE International Conference on Utility and Cloud Computing,2011

[4] Wael Alosaimi, Khalid Al-Begain," An Enhanced Economical Denial of Sustainability Mitigation System for the Cloud", Seventh International Conference on Next Generation Mobile Apps, Services and Technologies,2013

[5] Fahad Zaman Chowdhury, Mohd Yamani Idna Idris, Miss Laiha Mat Kiah, M A Manazir Ahsan," EDoS Eye: A Game Theoretic Approach to Mitigate Economic Denial of Sustainability Attack in Cloud Computing", 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC 2017), 4 - 5 August 2017, Shah Alam, Malaysia

[6] [6] Ahmad Shawahna, Marwan Abu-Amara, Ashraf S. H. Mahmoud, Yahya Osais, "EDoS-ADS: An Enhanced Mitigation Technique Against Economic Denial of Sustainability (EDoS) Attacks", IEEE Computer Society 2017