A SURVEY ON DETECTING DDOS ATTACK IN CLOUD ENVIRONMENT

[1]DrA.Somasundaram,[2]Dr.S.Devaraju,[3]Dr.S. Jawahar,[4]Dr.G.PrabuKanna,[5]Dr.M.Thenmozhi

[1]Assistant Professor, Department of Computer Applications, Sri Krishna Arts and Science College, Coimbatore,Tamil Nadu, India. somasundaram.a@gmail.com.

[2] School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh, India.devamcet@gmail.com

[3]Assistant Professor, School of Sciences, Christ deemed to be university, Delhi NCR, India.shivamjawahar@gmail.com

[4]Assistant Professor Grade2School of Computing Science and Engineering (SCSE),VIT Bhopal University, India.prabukanna.g@vitbhopal.ac.in.

[5]Assistant Professor,Dept. of Artificial Intelligence and Data Science,Sri Eshwar College of Engineering CoimbatoreTamil Nadu, India.thenmozhi.m@sece.ac.in

Abstract

Cloud computing is a prominent technology that offers a variety of services to its cloud users. Through the substantial growth of cloud computing, exchanging critical computing resources online motivates the researcher in creating new business models. Conversely, the adversaries use the technology to disrupt the deployed services offered by the cloud through a successful launch of (DDoS) Distributed Denial of Service attack, a major threat to cloud infrastructure by overloading the server with traffic to bring it to a halt. Creating monetary loss and a higher level of stress to the professionals are the direct ripple effects of service failure that can be circumvented by ascertaining DDoS attacks early before affecting the system. Unfortunately, DDoS attack is tremendously challenging to detect because of its stealthy nature. This paper surveys different contemporary techniques that detect DDoS attack in cloud-basedservices.

Keywords—Cloud computing; Stealthy nature; Distributed Denial of Service (DDoS) attack;

1. Introduction

Cloud technology enables the customers to access their customized services using virtualization technology over Internet. Cloud encompasses wide range of technologies from distributed computing to grid computing to offer measured, on-demand, cost effective, reliable service to the customers thru "Pay as You Go" model. Cloud rewords conventional business model by offering Infrastructure, Platform and Software services with highly extensible and auto scaling features. Cloud ensures guaranteed data and service availability using its fabricated features such as fault tolerant, load balancing, and redundant resources to reduce the service down time. According to survey [1], 94% of enterprises using cloud and 83% of enterprise will adapt to cloud by the year 2025.However, there is a reluctant in industry to deploy business in the cloud because of its security challenges. Cloud computing features such as multitenancy, on demand,auto-scaling, virtualization and resource sharing are associated with vulnerabilities and these can be exploited by the attacker to launch different types of attacks like Reduction of Quality (RoQ), privacy breachesand DDoSattacks.Distributed Denial of Service (DDoS) attack targets cloud environment and disturbs the availability of software and services to the benign user by maliciously consumption of computational and network resources. The DDoS attack is coordinated by DDoS agents and initiated in two stages of activity, namely the compromise phase and the attack phase. In compromise phase, the attacker identifies a system with vulnerability install malicious software or tools and converts the compromised machine as zombies. The attack phase, instruct the zombies to send volume of malicious requests to victim machine to drain it's computational and network resources [2].

Different verities of DDoS attacks like Data flooding, Attack on network devices, Protocol attack, Application attack, Operating system attack are launched to target the network, hardware or Application services by exploiting vulnerabilities associated in configuration or bug in device software [3]. When DDoS attack launched on the server, the cloud resource manager continues to allocate metered resources to maintain quality of service in accordance with service level agreements (SLAs). As a consequence of DDoS attack, request of legitimate user either denied or delayed due to scarcity of resource and this fraudulent consumption of metered resourcesresults in financial and business losses forSloud service Providers (CSPs) and their customers.

DDoS attacks can be directed in one of three waysto attack cloud environment such as consumption of unscalable resources, mutation of configuration and physical wipeout or transmutation of network components [17].The figure 1 depicts the impacts of DDoS attack in various layers of TCP/IP protocol suit.

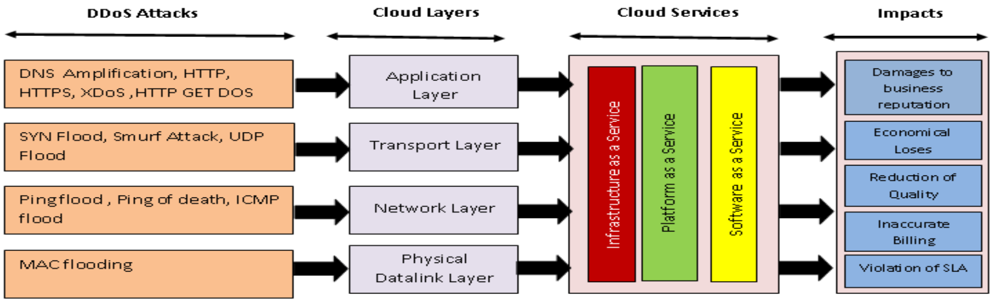

Fig.1. Impacts of DDoS attack

Numerous schemes have been proposed fordetect and mitigate DDoS attacks and most of them are inefficient due to heavy resource utilization, large operational cost, poor detection ratio due to dynamic changes in attack methodology and problems in deployment.This article examines various recent methods for detecting DDoS attacks in the cloud and presents a portrait of these methods.

2. DDoS Attack Detection

Attack detection is accomplishedby examine the attack symptomsthat are existsin cloud server in terms of its Service Level Agreements (ACL) and monitoring the performance using the metrics such as delayed response times,timeouts,and higher memory and CPU utilization. DDoS attack in cloud compromises the availability and deny the legitimate user from accessing the service. Attack detection is the process of classifying the normal and abnormal traffic. It is very hard to discriminate DDoS attack because of its stealthy nature, varying network traffic,dynamic attack signature and being launched in distributed manner [12]. The attackers keep on varying DDoS attack modes and methodology which form different DDoS variants such as Economic denial of sustainability and fraudulent resource consumption,Yo-Yo attack, energy DDoS attacks, Internal DDoS attacks/BotCloud, Collateral damage to nontargets, Power meltdown, Index page EDoS attack and Bandwidth DDoS attack [18]. The level of automation, explosion of vulnerabilities,frequency of attacks, and the impact of the attacks are used to categories DDoS attacks in a cloud environment. [20].

To detect the attack by inspecting each packet in network traffic is inefficient because of additional overload associated in processing and delayed response [8]. To counter the DDoS attacks number of IDS deploymentmodels likeHypervisor-based detection,Network-based detection systems and Host-based detection systems have proposed [14] , but they are inefficient in compacting complicated attackers. The attack detection requires continuous monitoring of traffic and sophisticated approach to classify the illegal requests. The Figure2 represents the phases involved in detecting DDoS attack.

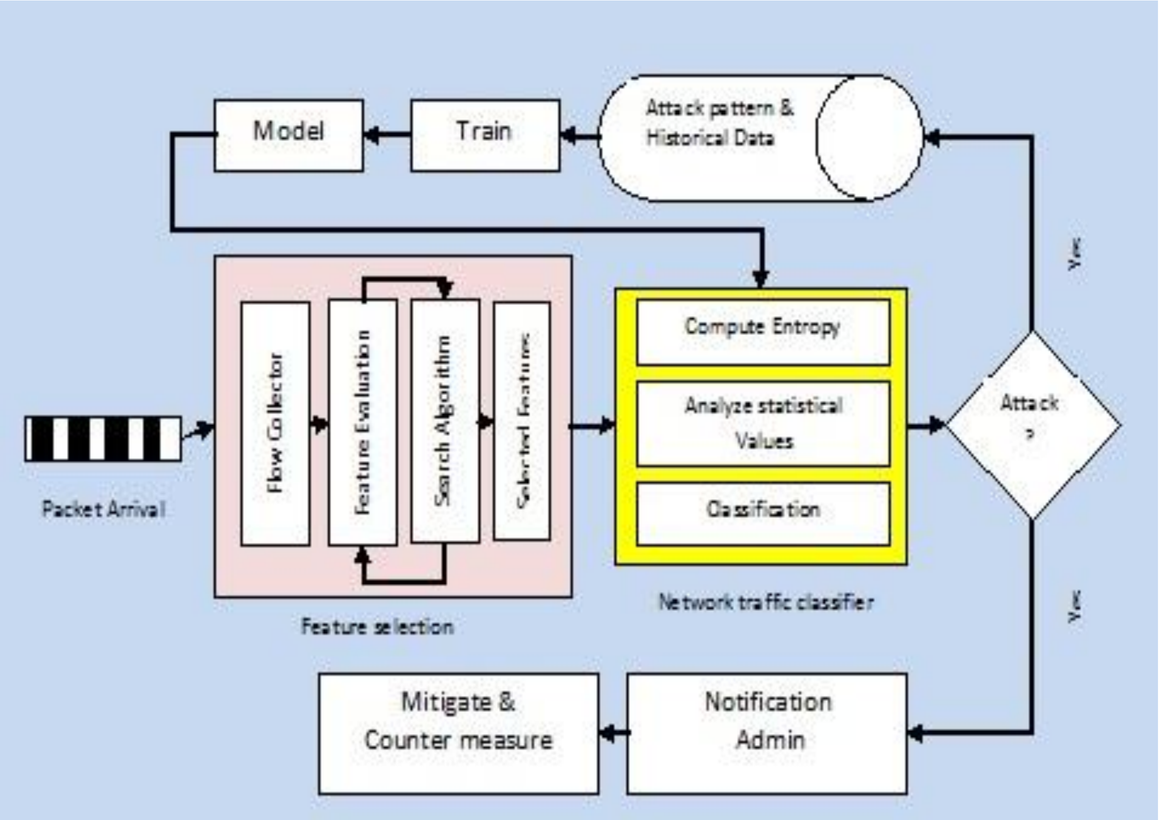

Figure2. Phases of DDoS Attack Detection

3.DDos detection taxonomy

Due to the frequency and impact of DDoS attack in cloud it takes wide attention of academic and industry researchers and numerous solutions have been proposed.

Signature-based detection

Signaturebased detection approach also known as Pattern detectionwhichrequires the prior knowledge on attack pattern and behavior. The incoming traffic is compared with exiting attack pattern using pattern matching algorithms to ensure the presence of attack instances. This method is not efficient because of rapid changes in attack pattern which is not available in pattern database [15].

Anomaly-based detection

Anomaly-based detection isan technique that realis on information theory. This approach analyzes the traffic behaviors and relates computed information with predefined threshold value which is updated dynamically. The deviation declares the presence of malformed instances in traffic.Due to varying nature of traffic and uncertainty of network it signals high false positive rate[16].

Hybrid

Hybrid approach integrates both Signature and Anomaly based attack detection. This approach have edge over than others in terms of detection rate, rapid identification of new signatures,lively update of ruleset, decreasing false positive rate and improved responses[21]

SDN Based Detection

SDN separates network devices control logic and data logic.The network's control plane, which is logically centralized and gives users a comprehensive overview of the network, also makes network hardware like switches and routers programmable. SDN abstracts the managed network and allows easily configuring and managing the network efficiently [19].

4. Related Work and Summary

To identify LDoS and HDoS in a connection-less environment, Hybrid Classifier based on Pattern of Arrival (HCPA) [4] was developed. The incoming traffic is extracted and an arrival pattern is formulated to classify the traffic by analyzing request arrival rate and pay load structure of the packet using clustering techniques. HCPA improves the accuracy of the detection rate in classifying abnormal UDP and ICMP traffic but not suitable for real time applications.

A framework for detecting DDoS attacks and clustering the victim VMs to recover them from attack was detailed by the author in the paper [5]. The attack was detected by continuously monitoring the number of connections established on VM and compared against with threshold values. In order to slow down the process and improve detection accuracy, the Self-Organized Mapping (SOM) based Neural Network (NN) is applied to cluster affected and non-attacked VMs.

The effects of DDoS attack were reduced by an anomaly-based framework [6]. Here the DDoS attack was detected using third party auditor (TPA).This frame work reduces the computational overhead of CSP and maintains the Service Level Agreement (SLA) of client by minimizing response time.

Collaborative approach for cloud computing [7] was proposed to detect and prevent DDoS attack. It uses Weibull distribution method to find out the identification factor left by the intruder. It mainly focus on detect spoofed IP and MAC address.

To identify both high-rate and low-rate attacks in cloud environment, a hybrid detection approach [8] was presented. This method determines the unique communication pair by computing the Shannon entropy of packet diversity H(z). The exponential moving average calculated using entropy values and total number of packets. The entropy value changes with great deviation depend on irregular patterns of real time applications. This variation is used to set the threshold value to filter the packet.

In order to increase overall detection accuracy and decrease detection delay, hybrid intrusion detection system (H-IDS) [9] was designed to identify DDoS attacks by merging the findings of both anomaly-based and signature-based detection approaches. This method is more suitable for the network which has varying traffic pattern.

Authors created the vote Extreme Learning Machine (V-ELM) classifier in [10] to use a majority vote technique to detect attacks in cloud networks.This proposed method applies machine learning approach to get the better performance in detection rate.

A confidence-based filtering method [11] was proposed to defend DDoS attack by utilizing correlation characteristics of traffic in attack and non-attack period. In order to determine whether to discard a packet or not, it determines the score of the packet, creates a relationship with attack period, and learns the system and traffic characteristics during non-attack periods

Karanbir Singh et al.[13] suggested T-CAD defense model for DDoS attack detection and mitigation by monitoring the edge routerofs in network. In order to distinguish between different types of traffic, T-CAD use information theory to determine the entropy of packets in a random period and compares it with different thresholds. It effectively identifies low- and high-rate DDoS attacks as well as flash events.

Table 1. Summary of various Detection Approach

	Detection Approach	Detection Parameter	Detection Metric	LDoS	HDoS	Mitigation Method	Approach	Real Time	Third Party Auditor	Data Set	Advantages	Drawbacks
HCPA [4]	Packet Arrival Pattern	Accuracy	Markov chain model	✓	✓	Filtering	Statistical	✗	✗	Simulated traffic data	- Low false positive rate	-Delayed response due to monitoring each packet
SOM based Clustering [5]	Normal threshold limit	Accuracy	Number of connections	✗	✓	Filtering	Machine Learning	✗	✗	Simulated traffic data	-Reduced Computational Cost	-Performance Issues
TPANGND [6]	Service Name	Performance	Response Time, Request rate	✓	✓	Filtering	Statistical	✓	✓	Real time Data	-Minimizes maintenance overhead	-Not suited for all CSP's
Cloud Warrior [7]	TCP , UDP ,ICMP Packets	Accuracy	Weibull distribution	***NA***	***NA***	Filtering	Statistical	✓	✓	Simulated traffic data	- Reduces cloud users Overhead	-Service delay

Hybrid detection method [8]	source IP address destination IP address	Accuracy	Exponential moving average (EMA)	✓	✓	Filtering & Rate Limiting	Statistical	✓	✗	Real time Data	- High reliability - High accuracy - Low false positive rate	-Not Adoptive to traffic changes
H-IDS [9]	Traffic density	Complexity	Multidimensional Gaussian mixture models (GMMs)	***NA***	***NA***	Rate Limiting	Anomaly & Signature-based	✗	✗	DARPA	- Requires low processing capacity	-Low performance in volumetric attack
V-ELM [10]	Majority Voting	Scalability	Moore Penrose inverse	***NA***	***NA***	Filtering	Machine Learning	✗	✗	NSL-KDD & ISCX	- Low computational cost	-Not Adoptive
Confidence-based filtering method [11]	Flow	Accuracy	Collaborative filtering	***NA***	***NA***	Filtering	Statistical	✗	✗	MAWI	- High level of accuracy	-Slow response
T-CAD	Flow	Accuracy	Normalized Entropy	✓	✓	Filtering & Rate Limiting	Statistical	✓	✗	Simulated traffic data	- Detect attack in early stages	-Need to inspect all the packet

5. CONCLUSION

There are numerous potential benefits associated with Cloud environment. However, due to System weakness, Outdated patches, Misconfiguration and Protocol vulnerabilities Cloud is easily targetable by DDoS attack. A comprehensive DDoS attack detection solution should have the capability of active learning to classify theattack in high speed and dynamically varying network traffic, early detection warrants to lower impacts of DDoS attack and cost effective and high performance in terms of accuracy and speed classifications.

REFERENCES

1. https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#1dc9c4dc6261
2. Singh, J., Kumar, K., Sachdeva, M. and Sidhu, N. DDoS Attack's Simulation Using Legitimate and Attack Real Data Sets. International Journal of Scientific & Engineering Research, 2012,volume 3, No. 6.
3. Mitrokotsa, A., Douligeris, C.: Denial of Service Attacks, Network Security:Current Status and FutureDirections, pp. 117–134.Wiley, Hoboken (2006)
4. V. Punitha and C. Mala, Traffic classification for connectionless services with incremental learning, Computer Communications (2019), doi: https://doi.org/10.1016/j.comcom.2019.11.017.

5. Nitesh Bharot, VeenadhariSuraparaju, and Sanjeev Gupt , DDoS Attack Detection and Clustering of Attacked and Non-attacked VMs Using SOM in Cloud Network , ICACDS 2019, CCIS 1046, pp. 369–378, 2019
6. Mahdavi Hezavehi, S., Rahmani, R. An anomaly-based framework for mitigating effects of DDoS attacks using a third party auditor in cloud computing environments. Cluster Comput 23, 2609–2627 (2020). https://doi.org/10.1007/s10586-019-03031-y
7. Saxena, R., Dey, S. DDoS attack prevention using collaborative approach for cloud computing. *Cluster Comput* **23,** 1329–1344 (2020). https://doi.org/10.1007/s10586-019-02994-2
8. P.D. Bojović, I. Bašičević, S. Ocovaj, M. Popović, A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method, Computers & Electrical Engineering, Volume 73, 2019, Pages 84-96, ISSN 0045-7906,https://doi.org/10.1016/j.compeleceng.2018.11.004.
9. ÖzgeCepheli, SalihaBüyükçorak, GüneşKarabulut Kurt, "Hybrid Intrusion Detection System for DDoS Attacks", Journal of Electrical and Computer Engineering, vol. 2016, Article ID 1075648, 8 pages, 2016. https://doi.org/10.1155/2016/1075648
10. Gopal Singh Kushwah , Virender Ranga, “Voting extreme learning machine based distributed denial of service attack detection in cloud computing” , Journal of Information Security and Applications , 53 (2020) 102532.
11. WanchunDoua,, Qi Chena, Jinjun Chen.” A confidence-based filtering method for DDoS attack defense in cloud environment”, Future Generation Computer Systems 29 (2013) 1838–1850.
12. R. Deka, D. Bhattacharyya, J. Kalita, DDoS attacks: Tools, mitigation approaches, and probable impact on private cloud environment, 2017, arXiv preprint arXiv:1710.08628.

13. KaranbirSingh ,Kanwalvir Singh Dhindsa , Deepa Nehra, “ T-CAD: A threshold based collaborative DDoS attack detection in multiple autonomous systems “ , Journal of Information Security and Applications 51 (2020) 102457
14. Omar Abdel Wahab, Jamal Bentahar, HadiOtrok, and Azzam Mourad,”Optimal Load Distribution for the Detection ofVM-based DDoS Attacks in the Cloud”, IEEE Transactions On Services Computing, DOI 10.1109/TSC.2017.2694426
15. Agarwal, B., & Mittal, N. (2012). Hybrid approach for detection of anomaly network traffic using data mining techniques. *Procedia Technology*, *6*, 996–1003. doi: 10.1016/j.protcy.2012.10.121
16. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58. doi: 10.1145/1541880.1541882
17. B. B. Gupta, Omkar P. Badve, “Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment”, Neural Computer & Applications (2017) 28:3655–3682
18. Gaurav Somani et.al, “Combating DDoS,,Attacks in the Cloud: Requirements, Trends, and Future Directions”,http://mycs.computer.org.
19. Diego Kreutz, Fernando M. V. Ramos, Paulo Ver´ıssimo, Christian Esteve Rothenberg, SiamakAzodolmolky, and Steve Uhlig. Software-Defined Networking: A Comprehensive Survey. CoRR, abs/1406.0440, 2014.
20. Akashdeep Bhardwaj et.al, DDoS Attacks, New DDoS Taxonomy and Mitigation Solutions – A Survey,International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016
21. Reddy SaiSindhuTheja, Gopal K. Shyam,An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment,Applied Soft Computing,Volume 100,2021,106997,ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2020.106997.