ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

A Productive DDoS TCP Surge Assault Identification and Aversion Framework in Cloud

P. Pritikha[1], S. Sruthi[2], M. Baskar[3]

UG Scholar, KCG College of Technology, Chennai, India[1,2]

Assistant Professor-Selection Grade, KCG College of Technology, Chennai, India[3]

ABSTRACT: Network security consists of the accession and protocols adopted to defend and administer unjustified access, dissipation, alteration, or elimination of a computer network and network-accessible resources. As DDoS flood attacks can be implemented in many forms, the form of these attacks cannot be foreseen. The cloud's virtual clients are under threat, and these threats increase as time passes. We present a new classifier system for detecting and preventing DDoS TCP flood attacks (CS_DDoS) in public clouds. The proposed CS_DDoS system offers a solution to securing stored records by classifying the incoming packets and making a decision based on the classification results. During the detection phase, the CS_DDOS identifies and determines whether a packet is normal or originates from an attacker. During the prevention phase, packets which are classified as malicious will be denied access to the cloud service and the source IP will be blacklisted. The performance of the CS_DDoS system is compared using the different classifiers of the least squares support vector machine (LS-SVM). The results show that CS_DDoS yields the best performance when the LS-SVM classifier is adopted.

KEYWORDS: Network Security, CS_DDoS, Detection, Prevention.

I. INTRODUCTION

Network security comprises of the procedure and schemesrecommended to preclude and monitor unapproved access, misappropriation, amendment, or denial of a computer network and network-accessible resources. Only network security can eliminate trojan horse viruses if it is triggered. Network security comrades with the endorsement of access to data in a network, which is controlled by the network administrator. Users opt or are assigned an ID and password or other certified information that allows them approach to information and curriculums within their authority. The Proposed System will help to reduce the DDoS attacks. The decided approach can efficiently improve the security of records, reduce bandwidth consumption and mitigate the exhaustion of resources. This system will reduce the financial loss occurring in organizations. The data will be safe and it cannot be accessed by unauthorized users. The attacker's IP address will be blocked and blacklisted.

II. RELATED WORK

Many detection and prevention methods for pacifying DDoS flood attacks have been proclaimed in the last few years. The rank correlation-based detection (RCD) scheme was intended. The creator of the RCD insisted that their scheme could discriminate whether the incoming requests were from legitimate users or from intruders. TheALPi algorithm suppressed difficulties in packet flows and improved utility by perpetuating the concept of packet enumeration. The ALPi therefore increases the detection certainty percentage and attack. Another DDoS attack deterrence architecture, known as secure overlay services (SOS) . The SOS architecture is a consolidation of three parts: secure overlay tunneling, routing via consistent hashing, and filtering. The authors claimed that the SOS can fortunately diminish the contingencyof these attacks using metastasize close to the secure edge and arbitrary close to the front edge.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

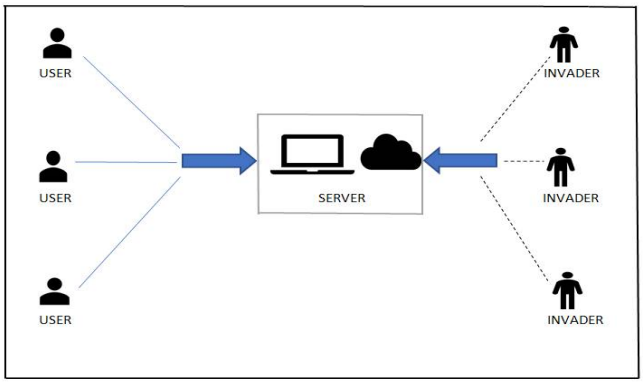
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

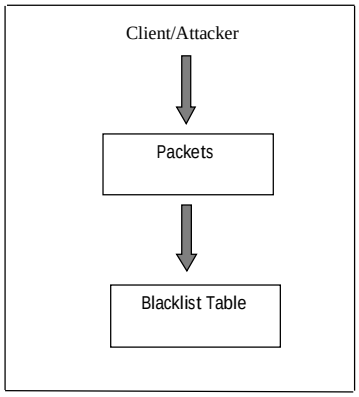
III. PROPOSED SYSTEM

The main goal of this system is to protect the data in the cloud from corrupting and to reduce DDoS attacks. Another goal is to prevent the bandwidth consumption and exhaustion of resources. Distributed denials of service (DDoS) assaults are the second most predominant cybercrime assaults after data robbery. DDoS TCP surge assaults can deplete the cloud's assets, expend a large portion of its data transfer capacity, and harm a whole cloud extend inside a brief timeframe. The guaranteeing of the accessibility and security of venture information, administrations and assets is as yet an urgent and testing research issue. We display a classifier framework for distinguishing and forestalling DDoS TCP surge assaults (CS_DDoS) in broad daylight mists. We present a new classifier system for detecting and preventing DDoS TCP flood attacks (CS_DDoS) in public clouds. The proposed CS_DDoS system offers a solution to securing stored records by classifying the incoming packets and making a decision based on the classification results.



PRE-PROCESSING MODULE:

It deals with the incoming packets sent by the user/intruder. The IP address from which the packet originated is compared with the IP addresses that are present in the black list table which is updated regularly. If the packet is an abnormal packet from a new IP address, then it is immediately blacklisted and updated in the black list table.



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

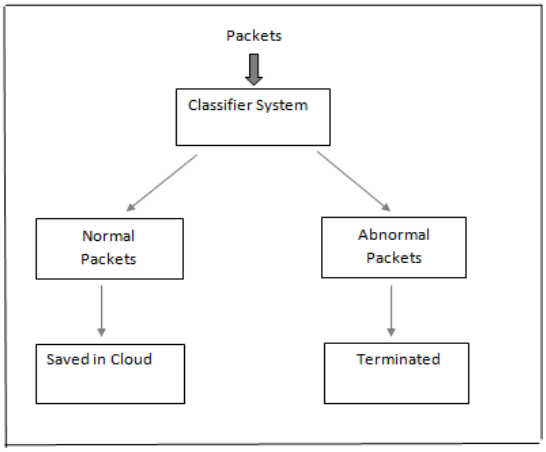
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

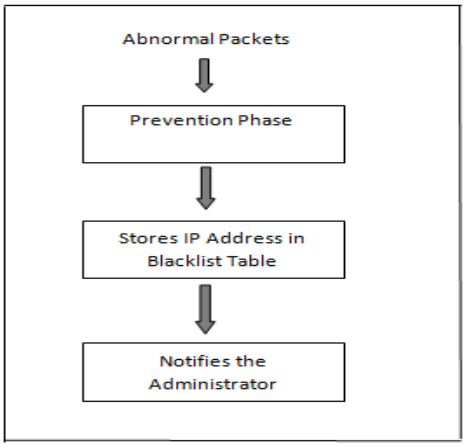
DETECTION PHASE MODULE:

If the IP address from which the packet originated does not match with the set of IP addresses in the black list table, then it comes to the detection phase. In the detection phase, the packet is classified as normal or abnormal based on the TCP header packet size, threshold value and the timeframe. If it is a normal packet it is allowed to store in the cloud, if not it then goes to the next phase.



PREVENTION PHASE MODULE:

After the classification of packets in the detection phase, if it is an abnormal packet it arrives to the prevention phase. In the prevention phase the following steps are taken to safeguard the cloud and the server from the abnormal packet. As soon as it is found out to be an abnormal packet it is blocked and the IP address from which it originated is blacklisted. Identification of abnormal packets leads to notifying the administrator immediately.



ALGORITHM USED

Step 1:
There are two parameters in the algorithm,
δ -Common threshold value
C - Threshold value of arriving packets

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

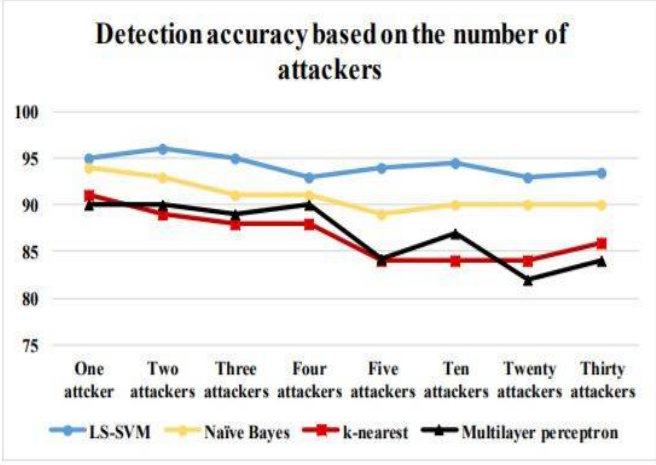
Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018

ΔT- Sampling interval
These three parameters are initialized in the first step
Step 2:
The flow at which the packet arrives is identified and initially the count number of each flow is set to 0.
x1=x2=…….=xn=0
Step 3:
After the specified ΔT is over, the threshold value of the arrived packets are calculated.
Step 4:
The threshold value of each flow f1,f2,…..fn is stored.
Step 5:
If the threshold value C1,C2,….Cn of the packets with flow f1,f2,……fn is equal to the common threshold value δ , then the packet can be allowed to store in the cloud.
Step 6:
If the threshold value C1,C2,….Cn is not equal to the common threshold value δ, then packet is discarded.
Step 7:
When new packets arrive, the algorithm is repeated from step 2.

IV. RESULTS AND CONCLUSION

The proposed system shows that using LS-SVM the CS_DDoS system can identify the attacks accurately. Thus, the proposed approach can efficiently improve the security of records, reduce bandwidth consumption and mitigate the exhaustion of resources. The blocking of malicious packets safeguards the cloud from data loss or corruption.



The above graph depicts the accuracy of detecting the attackers using LS-SVM.

The web application that is built finds the DDoS attack with 97% accuracy by classifying the packets as normal and abnormal packets using the LS-SVM algorithm.

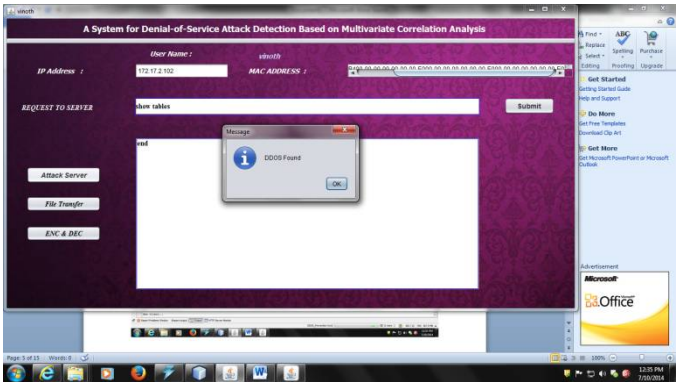
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Special Issue 4, April 2018



The above image depicts the DDoS attack that was found when an attacker tried to crash the server by flooding it with packets. The attacker is identified and blocked. An alert message is sent to the administrator about the DDoS attack and the attacker.

REFERENCES

[1] Girma, K. Abayomi, and M. Garuba, "The Design, Data Flow Architecture, and Methodologies for a Newly Researched Comprehensive Hybrid Model for the Detection of DDoS Attacks on Cloud Computing Environment," in Information Technology: New Generations, ed.: Springer, 2016, pp. 377-387.
[2] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, "The economic impact of cyber-attacks," Congressional Research Service Documents, CRS RL32331 (Washington DC), 2004.
[3] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges," IEEE Communications Surveys & Tutorials, vol. 18, pp. 602-622, 2016.
[4] P. A. Laplante, J. Zhang, and J. Voas, "What's in a Name? Distinguishing between SaaS and SOA," It Professional, vol. 10, pp. 46-50, 2008.
[5] C. Balding, "What everyone ought to know about cloud security," ed., http://www.slideshare.net/craigbalding/what-everyone-oughtto-know-about-cloud-security, 2012. [6] E-CrimeCongress.E-CrimeSurvey, /http://www.ecrimecongress.org/ecrime2009/documents/eCrimeSurvey2009_AKJ_KPMG(1).pdfS 2009. [7] B. Wang, Y. Zheng, W. Lou, and Y. T. Hou, "DDoS attack protection in the era of cloud computing and software-defined networking," Computer Networks, vol. 81, pp. 308-319, 2015.
[8] M. Xia, W. Lu, J. Yang, Y. Ma, W. Yao, and Z. Zheng, "A hybrid method based on extreme learning machine and k-nearest neighbor for cloud classification of ground-based visible cloud image," Neurocomputing, vol. 160, pp. 238-249, 2015
[9] A. Taravat, F. Del Frate, C. Cornaro, and S. Vergari, "Neural networks and support vector machine algorithms for automatic cloud classification of whole-sky ground-based images," IEEE Geoscience and remote sensing letters, vol. 12, pp. 666-670, 2015.
[10] A. Sahi, D. Lai, and Y. Li, "Security and privacy preserving approaches in the eHealth clouds with disaster recovery plan," Computers in Biology and Medicine, vol. 78, pp. 1-8, 2016.
[11] A. Sahi and D. Lai, "Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol," in Telecommunications (ICT), 2015 22nd International Conference on, 2015, pp. 204- 208.
[12] A. Sahi, D. Lai, and Y. Li, "Parallel encryption mode for probabilistic scheme to secure data in the Cloud," in 10th International Conference on Information Technology and Applications (ICITA), Sydney, 2015