Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN : 2348-4470
p-ISSN : 2348-6406

International Journal of Advance Engineering and Research Development

Special Issue on Recent Trends in Data Engineering

Volume 4, Special Issue 5, Dec.-2017

Securing Cloud Server from DDoS Attack

Minal Nerkar[1],MayurHiwarkar[2],Kunal Parkar[3], Sukirti Singh[4] , Rutuja Butle[5]

[1]*Computer Engineering, AISSMS IOIT*
[2]*Computer Engineering, AISSMS IOIT*
[3]*Computer Engineering, AISSMS IOIT*
[4]*Computer Engineering, AISSMS IOIT*
[5]*Computer Engineering, AISSMS IOIT*

Abstract—*A distributed denial-of-service (DDoS) is where the attack source is more than one, often thousands of unique IP addresses. Flooding is one of the typical DDoS attacks that exploit normal TCP connections between a client and a target web server. In this project we are trying to devise a DDoS anomaly detection method on cloud that implements a data mining detection algorithm against the Flooding attacks.Detection of DDoS Attack is a basic measure towards defense. DDoS attacks may result in system performance degradation of the targeted network, which can cause the services intended to the genuine users not in function or may produce delayed results.In this project we will detect a real-time DoS attack from a number of machines on the live cloud and allow the genuine users to access the service without any lag and block the bad user and prevent the DDoS attack.*

Keywords- *DDoS, Data Mining, Cloud Computing, Network Bandwidth, Bot Net, HTTP Gate Attack, Flooding Attack, Cloud.*

I .INTRODUCTION

Project Idea

In our project we aim to secure the cloud from evolving DDoS attacks using Data Mining techniques. The algorithm used for this is kNN(k-Nearest Neighbor) algorithm. We aim to mitigate the attack at run-time thus blocking the malicious user from accessing the services of the cloud. The attack under consideration is HTTP GET attack. Whenever the malicious user attacks the cloud, our system will detect the attack pattern from a host of parameters viz. Timestamp, Port number. and then block the user and update the IP of the attacker to a table and if the service request is made from that particular IP again, then our system will deny that request thus clearing the path for the good user for the uninterrupted service.

Motivation of the Project

Criminal perpetrators of DoS and DDoS attacks often target sites or services hosted on high-profile web servers such as banks, credit card payment gateways. Motives of revenge, blackmail or activism can be behind other attacks.
The United States Computer Emergency Readiness Team (US-CERT) defines symptoms of denial-of-service attacks to include:

- Unusually slow network performance (opening files or accessing web sites)
- Unavailability of a particular web site
- Inability to access any web site

II.RELATED WORK

Earlier, the methods to detect and mitigate the DoS attacks were available. But coming age attacks were much more brute and it involved 1000's of systems being attacked at once. To track them were a tedious task. Some of the methods to detect and mitigate DoS attacks were even useful as they could detect the attacks even before it happened. But those methods cannot be applied for DDoS as it much more large in scale. The recent attack of Ransomware virus took place which blocked the access of millions of users around the globe. The attack was neutralized after a patch was released to mitigate it.

III. PROPOSED ARCHITECTURE

A description of the program architecture is presented. The block below represents a Cloud and the entities inside the block are the components of the cloud. The different data nodes in the figure indicate various servers on the cloud. For ex. : MySql

port, MongoDB port which can be targeted by the attackers.

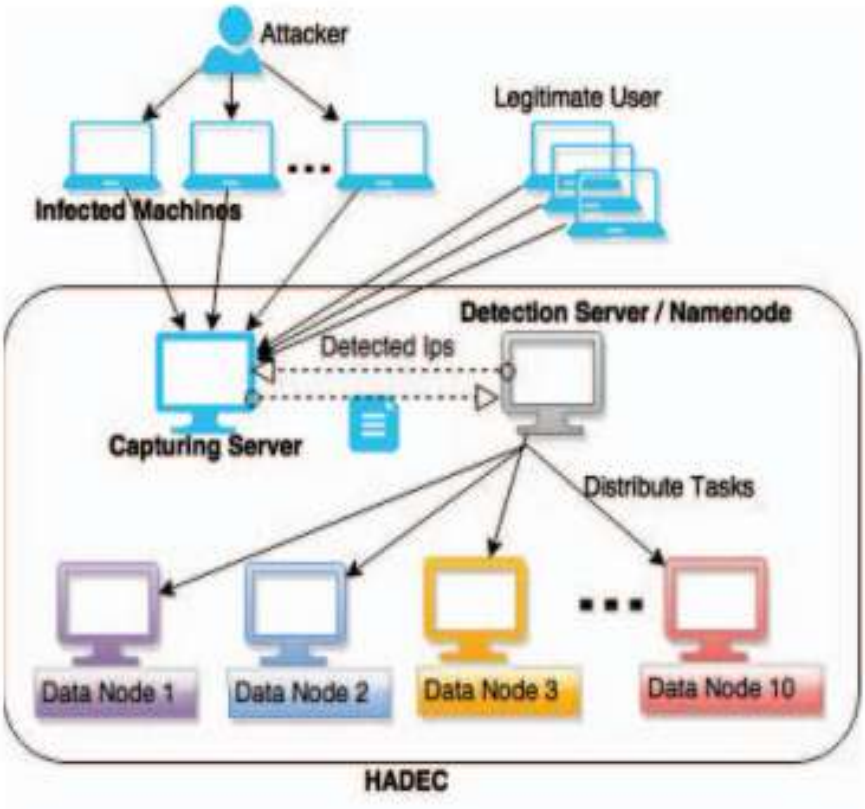

Fig. 1 Proposed Architecture of Scheduling of Containers.

IV.ALGORITHM

kNN algorithm provides simplicity, effectiveness and intuitiveness in the further determining the result. Also it is robust to noisy training data and is effective when the training dataset is high which shadows the disadvantages of Naïve Bays algorithm .Our project contains a set of dataset which are interdependent on the each other and Naive Bays works on the data which is dependent. So Naïve Bays is not suitable for our project. Hence we will be using the kNN algorithm which is very robust and provides the output very quickly.

Input Parameters: Set of all Ports and IPs
Output: Log Files, Attacker IP Details
Step 1: Store all the training tuples.
Step 2: For each unseen tuple which is to be classified.
A. Compute distance of it with all the training tuples using Euclidean Distance.
B. Find the k nearest training tuples by use N-dimension form of the Euclidean distance.
Step 3: Compute set of live data IP using TCPDUMP commands.
Step 4: Analyze the data collected.
Step 5: Mitigate the attacker and update the IP table.
End for

Mathematical Model:
Input:
Let ‘S’ be the
S= {D1, D2}
Where,
D1: {Set of Live data IP TCPDUMP}
D2: {Set of All Ports and IPS}

Output:
O = {D, L, A}
D= {Attacker IP Details}
L= {log files}
A= {alerts}

Function:
S= {F1, F2, F3, F4}
F1= {Data collection}
F2= {Analysis}
F3= {Mitigating}
F4= {IP Table Update}

- *Success Conditions :* Attacker Mitigated
- *Failure conditions :* Error message for failure

V. APPLICATIONS

Data sensitive Items :

- Banks
- Railway Reservation
- Government Schemes(AAdhar).
- College's Exam Cloud Server

VI. CONCLUSION AND FUTURE SCOPE

Our paper aims at developing such a system that will help in securing cloud server from emerging DDoS attack. The main intention of DDoS attacker is to deprive the good user from accessing the services from server on cloud by flooding malicious packets on the network line thus , making the server busy We have used kNN algorithm for differentiating between the good user and bad user by analyzing factors like source IP, destination IP, port number and timestamp.Preventing the DDoS attacks will allow the genuine users to use the service uninterruptedly. Detecting the DDoS attack at real time will help to prevent the attack in future. Securing the cloud environment can be achieved, which is very important for uninterrupted services used in Banks,Railway Reservation ,Government Schemes(AAdhar).

VII. REFERENCES

[1] Preeti Daffu, Amanpreet Kaur, "Mitigation of DDoS attacks in Cloud Computing," 5th International Conference on Wireless Networks and Embedded Systems (WECON), pp. 01-05, 2016.
[2] Jeanette Smith-Perrone, Jeremy Sims, "Securing Cloud ,SDN and a Large Data Networks Environments from Emerging DoS Attacks," 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, pp. 466-469, 2017.
[3] Jin Tang, Yong Hao, Wei Song, "SIP Flooding Attack Detection with a Multi-Dimensional Sketch Design," IEEE Transactions on Dependable and Secure Computing, Vol.11, Issue 6, pp. 582-595, 2013.
[4] Anand Keshri, Mayank Agarwal, Sunit Kumar Nandi, "DoS attacks Prevention using IDS and Data Mining," 2016 International Conference on Accessibility to Digital World (ICADW), pp. 87-92, 2016.
[5] Johan Sharif, Mudrik Alaydrus, " Building a private Cloud Computing and the analysis against DoS (Denial of service) attacks," 4th International Conference on Cyber and IT Service Management, pp. 01-06, 2016.
[6] Shiu Yu , Yonghhong Tian, Song Guo, "Can We Beat DDoS Attacks in Cloud?," IEEE Transactions on Parallel and Distributed Systems, Vol. 25, Issue 9, pp. 2245-2254, 2014.
[7] Mais Nijim, Mohannad Khan, " FastDetict: A Data Mining Engine for predecting and preventing DDos Attacks," 2017 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 01-05, 2017
[8] Nikhil Tripathi , Neminath Hubbali, "How Secure are web Servers?An Empirical Study of slow HTTP DoS Attacks And Detection", 11th International Conference on Availability, Reliability and Security (ARES), pp. 454-463, 2016
[9] K.Muthupriya, Dr.S.Mercy Shalinie, Mr.K.Narasimha Mallikarjunan, "A servey of Distributed Denial of Service attack", 10th International Conference on Intelligent Systems and Control(ISCO), pp. 01-06, 2016, 2016
[10] Yeonhee Lee, Young seok Lee, "Detecting DDoS Attacks with Hadoop", ACM CoNEXT Student Workshop Japan, 2011

