ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

DDoS Detection and Prevention in Cloud with Dynamic Dataset and Artificial Intelligence for Intrusion Detection System

Monalisa A. Shinde, Shripadrao Biradar

Research Scholar, Department of Computer Engineering, RMD Sinhgad School of Engineering, Warje, Pune, India

Assistant Professor, Department of Computer Engineering., RMD Sinhgad School of Engineering, Warje, Pune, India

ABSTRACT: A cloud provides different services and made them available. So cloud performs a vital role in information technology. It has many advantages. But now days, security of cloud is a major issue. DDoS attack on cloud is a big threat. To avoid and minimize DDoS attack various techniques are evolved. Usually a cloud has profound resources, full control over that resources and dynamic allocation capability for them.Therefore, cloud has the potential to overcome DDoS attacks. However, individual cloud hosted servers are still vulnerable to DDoS attacks if they run in the traditional way. The proposed system tries to detect and prevent DDoS attack on cloud. It uses an intrusion prevention system which has capability of creating a dynamic dataset. System extracts some features of every request coming to the server. Then it applies artificial intelligence and predicts whether it is a request from legitimate user or attacker. If it is from attacker then it do not process request and update log. And if request is from legitimate user then it applies requested algorithm, send response and update log. So it offers a way to counter DDoS attacks against individual cloud customers.

KEYWORDS: Cloud computing, Distributed Denial of Service Attack, Software as a Service, ICMP, DNS

I. INTRODUCTION

Now a days, Cloud is a best and a dominant computing platform. A cloud provides different services and made them available. It operates on the basis of pay-as-you-go. So cloud performs a vital role in information technology. It has some advantages and limitations. And DDoS attack is now a major issue. To avoid and minimize DDoS attack various techniques are evolved.

A. *Cloud Computing:*

Cloud computing are classified on the basis of services it provides and its various deployment models. On the basis of various types of offered services, it can be considered consisting of three layers. Infrastructure as a Service (IaaS) is the bottom most layer which provides basic infrastructure services. The middle layer is Platform as a Service (PaaS) layer. It provides platform oriented services; moreover it also provides the environment for user applications. The upper most layer is Software as a Service (SaaS). It provides the various applications as demanded.

SaaS guarantees the whole applicationsare presented on the Internet. And it also guarantees that users can use them properly. The payments are issued on the basis of pay per use model. By this, main burden of installation of software, running it and also maintaining that on client's computer is removed completely. In SaaS, two types of servers are used. First is called as Main Consistence Server (MCS) and second is called as Domain Consistence Server (DCS). Both cooperate to achieve cache coherency. If MCS is scratched, or negotiated, the control over the cloud environment is gone. So MCS must be secure.

B. *Denial of Service Attacks:*

A DoS attack is an attempt to make the resources and services to the authorized normal users unable which are used by them. In these attacks, the server which is providing the service is flooded by a very large number of re-

DOI: 10.15680/ijircce.2015.0306128

quests. Hence the service becomes unavailable to legitimate user. The DoS attack increases consumption of bandwidth, causes congestion, makes some parts of the clouds inaccessible to the legitimate users.

C. *Distributed Denial of Service Attacks:*

DDoS is generally called as an advanced version of DOS. In this attack also large number of packet are sent to the victim server so that services running on a server will be denied to legitimate user. But on contrast to DoS, DDoS attack is run by three units: Master, Slave and Victim. Master launches the attack but slave is the network which acts like a launch pad for master. So this is also called as co-ordinated type attack.

A DDoS attack makes the service unavailable to the legitimate usersimilar way to the DoS attack but different in the way of launching. A DDoS attack mainly operates in two steps: first one is Intrusion phasein which Master tries to compromise less important machines to use flooding. In second step it installs DDoS tools and makes attack the victim server.

II. RELATED WORK

Author D. K. Y. Yau et al. [1] treated DDoS attack as a resource managementproblem. The major issue in this is to allocate extra resources to system, there is issue that how detection algorithms and filtering algorithm worksand what's there accuracy is. Researchers Shui Yu and Yonghong Tian et al. [2] suggested that clone the sufficient intrusion prevention servers immediately filter out attack packets.This guarantees the quality of the service for legitimate users. To minimizeDDoS attack extra reserved resources are allocated. System dynamicallyallocates resource to targeted customers of individual cloud. Also provide an Intrusion Prevention System (IPS) at various access points which are placedin internet and cloud. All incoming packets will be monitored by this IPS. Whenever a DDoS attack is experienced by system, this mechanism will allocate extra reserved resources. And a resource pool will maintain thetrack of all reserved resources.Based on the strength of the packets coming, system clones new virtual machines depending on the different image files of IPS. These all IPS together try to drop attack packets. When DDoS becomes less effective, automatically IPS of system will be dismissed and the virtual machine also dismissed onwhich the IPS is located which in turn releases the extra resources allocated from pool.

Researchers R. Bhadauria et al. [3], M.A. Rajab et al. [4], T. Peng et al.[5] suggested that DDoS attack is just a competition for resources and thewinner is the side who possesses more resources. The most harmful DDoSattack can be minimized by using cloud platform itself. A mechanism calleddynamic resource allocation has ability to allocate all the available resources dynamically. So this system uses this mechanism which automatically willcoordinate with all the available resources in the cloud. This will minimizethe DDoS attacks on customers of individual cloud. But the problem becomesmore tedious if the system which employs dynamic allocation fails.Researchers M. Armbrust et al. [6] proposed that when a DDoS attackoccurs, system employ the idle resources of the cloud. But if sufficient idealresources are not available in system then it becomes difficult to overcome DDoS attack node.

III. SCOPE OF RESEARCH

To develop a strategy to get the prediction about type of request to deliver service to normal cloud customer with prevention to attacker request and to counter DDoS attacks against individual cloud customers.

IV. PROPOSED SYSTEMFRAMEWORK AND DISCUSSION

A. *System Architecture:*

The figure 1 shows, the system architecture of proposed system. It mainly contains an individual cloud server serving a normal user. A normal user has a set of images which he needs to convert into some other forms. There are three operation namely, gray scale, threshold and blur. Normal user sends request server to convert the image into one of these formats. In this system there is an attacker who tries to launch DDoS attack on the system. For this he creates two agents and these two agents send multiple requests to server repeatedly so that server should get busy in responding these and normal user will not get server's service properly.

DOI: 10.15680/ijircce.2015.0306128

But for every request, server first extracts some features from it. Then apply artificial intelligence algorithm. And predict whether its attacker's request or normal user's request. If it's attacker request then server don't allocate resources to it. If it's normal user's request server applies requested image processing algorithm. And send response to the normal user.

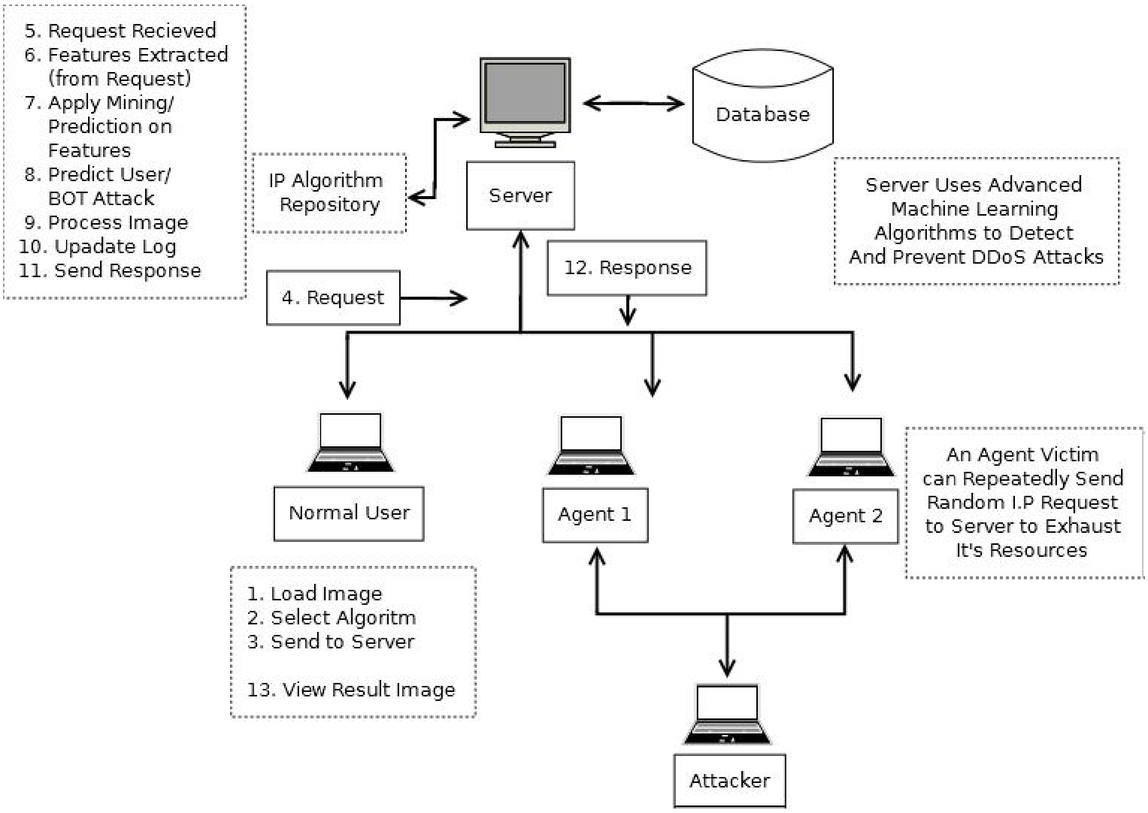
5. Request Recieved
6. Features Extracted (from Request)
7. Apply Mining/ Prediction on Features
8. Predict User/ BOT Attack
9. Process Image
10. Upadate Log
11. Send Response
IP Algorithm Repository
Server
Database
Server Uses Advanced Machine Learning Algorithms to Detect And Prevent DDoS Attacks
4. Request
12. Response
Normal User
Agent 1
Agent 2
An Agent Victim can Repeatedly Send Random I.P Request to Server to Exhaust It's Resources
1. Load Image
2. Select Algoritm
3. Send to Server
13. View Result Image
Attacker

Figure 1. System Architecture

B. *Algorithms:*

i) *Algorithm 1: ServerAlgorithm:*

In server algorithm, when client sends request, that request is analyzed and some features are extracted. Anartificial intelligencealgorithm isthen applied to make prediction about the request type. According to result output is delivered to normal user only.

Input: Request from client

Output: Prediction of request type and response to normal user

```
Server algorithm( )
Step 1. {
Step 2.    receive request();  _
Step 3.    IP req.IP();
Step 4.    currTime  = getSystemTime();
Step 5.    diffTime = findLastrequestIP();
Step 6.    passToANN();
Step 7.    Apply the artificial intelligence algorithm  (ANN)
Step 8.    ShowResult();
Step 9.    ifcurrReq == attackerReq
Step 10    {
```

DOI: 10.15680/ijircce.2015.0306128

```
Step 11.      Stop processing;
Step 12.   }
Step 13.   else
Step 14.   {
Step 15.      Pass to requested image processing algorithm
Step 16.      Send result
Step 17.    }
Step 18.   Return
Step19.  }
```

ii) Algorithm 2: Artificial intelligence algorithm (ANN)

An artificial intelligence is used in this system to make prediction about the request type. Artificial Neural Network (ANN) algorithm is used for this purpose. Forward propagation is first applied to train the neural network. Then error are alsocalculated and corrected in network. Afterwards, for each request, extracted features are passed as input to ANN. Finally it gives result that whether it'sattacker's request or normal user's request.

Input: Extracted features
Output: Prediction of request type

```
Forward  Propagation()
Step 1. {
Step 2.    Input  nodes i, given input  x_i:
Step 3.    For each input  node i_
Step 4.    Output_i = x_i
Step 5.    Hidden layer nodes j
Step 6.    For each hidden neuron j
Step 7.    Output_j = ∑phi(w_ji.output i)
Step 8.    Output layer neurons k
Step 9.    For each output neuron k
Step 10.   output k = ∑ phi(w_kj.output_j)
Step 11.}

Activate  Layer(input,output)
Step 1. {
Step 2.    for each i input  neuron
Step 3.        calculate  output i
Step 4.    for each j hidden neuron
Step 5.        calculate  output j
Step 6.    for each k hidden neuron
Step 7.        calculate  output k
Step 8.    output = output k
Step 9. }
```

iii) Algorithm 3: Gray scale algorithm

Gray scalealgorithm is used to convert anormal imageto the gray scale image.

Input: Normal image
Output: Gray scale image

```
Gray scale( )
Step 1. {
Step 2.    for Each Pixel in Image
Step 3.    {
Step 4.       Red = Pixel.Red
Step 5.       Green = Pixel.Green
Step 6.       Blue = Pixel.Blue
Step 7.       Gray = (Red + Green + Blue) / 3
Step 8.      Pixel.Red  = Gray
Step 9.      Pixel.Green  = Gray
Step 10      Pixel.Blue = Gray
Step 11.   }
Step 12. }
```

iv) Algorithm 4: Threshold algorithm

Threshold algorithm is used to convert a normal image to the threshold image. For this, user must have to select the threshold and then that threshold is used to convert the image.

Input: Normal image

Output: Threshold image

```
Threshold( )
Step 1. {
Step 2.    for i = 0 to height
Step 3.    {
Step 4.      for j = 0 to width
Step 5.      {
Step 6.        if Pixel < threshold
Step 7.            Then pixel = 0
Step 8.        else
Step 9.            pixel = 255
Step 10      }
Step 11.   }
Step 12.}
```

v) Algorithm 5: Blur algorithm

Blur algorithm is used to convert a normal image to the blur image.

Input: Normal image

Output: Blur image

```
Blur( )
Step 1.  {
Step 2.    Traverse through entire input image array
Step 3.    Read individual pixel color value (24-bit)
Step 4.    Split the color value into individual R, G and B 8- bit values
Step 5.    Calculate the RGB average of surrounding pixels and assign this average value to it
Step 6.    Repeat the above step for each pixel
Step 7.    Store the new value at same location in output image
Step 8.  }
```

V. RESULT SET

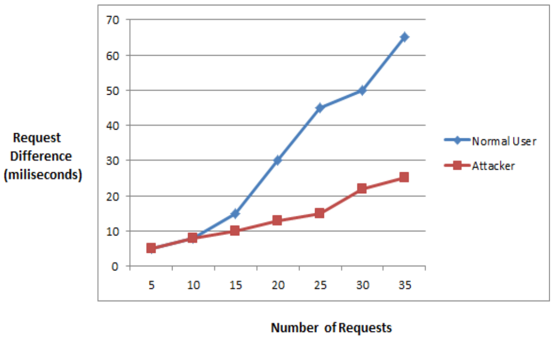

Figure 2. Analysis of Artificial Intelligence Algorithm

As shown in figure 2, artificial intelligence algorithm is analyzed. This graph shows the parameter number of requests on X-axis and request difference on Y-axis.Whenever request difference between the current and last request of same IP address is very less, mostly artificial algorithm declares the request as an attacker`s request. On the other hand, when request difference is less then it declares that request as a normal request.Therefore, attackers graph line is very close to X-axis as it has very less request difference. Whereas, graph line of normal user is in upward direction as request difference for normal user is very large as compare to attacker.

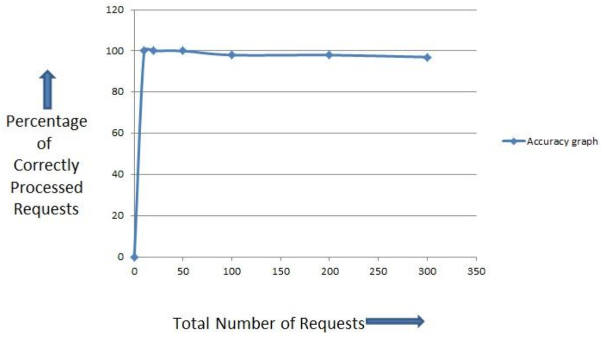

Figure 3. Accuracy Graph

Figure 3, shows accuracy graph of the system. X-axis of accuracy graph represents total number of requests, while Y-axis represents percentage of the correctly processed requests. First 10 requests are sent to the system and response of system is analyzed. Then it is observed that system gives accurate result for all requests i.e. accuracy is 100%. Then 20, 50, 100, 200 and 300 requests are sent respectively. It is observed that system gives accurate result for 100%, 100%, 98%, 98% and 97% requests. As shown in graph, system gives 100% accuracy many times. But slowly accuracy decreases as number of requests goes more than 100. But still overall system accuracy remains very close to the 100%.

VI. Conclusion and Future Work

In this system, whenever request comes, system extracts few important parameters of request like IP address, current time, size of image and request difference. Then system passes these parameters to intrusion prevention system which uses dynamic datasets. Intrusion prevention system applies artificial intelligence algorithm to these parameters and dataset. Then it predicts which type of request is this.If request is an attack request then it don't send any response to the attacker and update the database of system. But if request is a legitimate request then send it for next processing like image processing algorithms.At last, each legitimate user will get results its converted image. And so it can prove that DDoS attack is overcome successfully. In future, this intrusion prevention system can be replicated on the basis of DDoS attack measurement.

Future enhancement of the system is to add more parameters in artificial intelligence algorithm to make more strong prediction about the type of request. Also, intrusion prevention system of proposed system can be replicated on the basis of DDoS attack measurement.

References

1. D. K. Y. Yau, J. C. S. Lui, F. Liang, and Y. Yam, “Defending Against Distributed Denial-of-Service Attacks with Max-Min Fair Server-Centric Router Throttles”, IEEE/ACM Trans. Netw., vol. 13, no. 1, pp. 29-42, Feb. 2005.
2. Shui Yu, Yonghong Tian, Song Guo, Dapeng Oliver Wu, “Can We Beat DDoS Attacks in Clouds?”, IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 9, September 2014.
3. R. Bhadauria, R. Chaki, N. Chaki, and S. Sanyal, “A Survey on Security Issues in Cloud Computing”, CoRR, vol. abs/1109.5388, 2011.
4. M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “My Botnet is Bigger Than Yours(Maybe, Better Than Yours): Why Size Estimates Remain Challenging”, in Proc. 1st Conf. Hot Bots, 2007, p. 5.
5. C. Peng, M. Kim, Z. Zhang, and H. Lei, “Vdn: Virtual Machine Image Distribution Network for Cloud Data Centers”, in Proc. INFOCOM, 2012, pp. 181-189.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

6. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing”, EECS Dept., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, Feb. 2009.
7. M. Chowdhury, M. Zaharia, J. Ma, M. I. Jordan, and I. Stoica, “Managing data transfers in computer clusters with orchestra”, in SIGCOMM, 2011.
8. S. Subashini and V. Kavitha, “A survey on Security Issues in Service Delivery Models of Cloud Computing”, J. Netw. Comput. Appl., vol. 34, no. 1, pp. 1-11, Jan. 2011.
9. J. Francois, I. Aib, and R. Boutaba, “Firecol, a Collaborative Protection Network for the Detection of Flooding DDoS Attacks”, IEEE/ACM Trans. Netw., vol. 20, no. 6, pp. 1828-1841, Dec. 2012.

BIOGRAPHY

Monalisa Shinde is Research Scholar RMD Sinhgad School of Engineering Pune, University of Savitribai Phule, Pune. She received B.E. in Computer Engineering from S. S. V. P. S. B. S. Deore’s College of Engineering, Dhule form North Maharashtra University, Jalgaon. Currently she is perusing M. E. in computer engineering from R. M. D. Sinhgad School of Engineering, Pune, University of Savitribai Phule, Pune.

S. S. Biradar is working as Assistant Professor of Computer Engineering Department in RMDSSOE Pune, India. He received the B.E. degree in Computer Scienceand Engineering from PDACOE Gulbarga Karnataka andM.E. degree in DCN from Dr. AIT Banglore Karnatakain 2010 and 2012 respectively.

DOI: 10.15680/ijircce.2015.0306128