SECURITY IN CLOUD COMPUTING ENVIRONMENT

Mrs. Radhika B[1], Abhishek Sharmait[2], Dhairay Ahujait[3], Arun Kr Dubey[4]

[1]Academic Officer (ICT), National Institute of Open Schooling, Noidaradhika.nios@gmail.com
[2]Bharati Vidyapeeth's College of Engineering, New Delhi, Indiasharmaabhishek848@gmail.com
[3]Bharati Vidyapeeth's College of Engineering,New Delhi, Indiadhiru21@gmail.com
*[4]*Corresponding Author, Bharati Vidyapeeth's College of Engineering,New Delhi, Indiaarudubey@gmail.com*

Abstract

The new term in computer based services and in IT industry is cloud computing. Because of its numerous challenges like availability, security, performance etc it is still in its infancy. Since the infrastructure of cloud computing is potentially shared by millions of users, DDOS attack have become a major threat to cloud computing where it is preventing the users to use cloud infrastructure services and these kind of attacks can be made by legitimate and illegitimate cloud users. Thus it is becoming the main disrupt in cloud operations.

In this paper first we will introduce cloud along with the challenges faced by cloud environment. Then brief about DDoS along with its classifications and defence mechanism. At last we will discuss our followed approach.

Key Words: *- Cloud Computing, On demand Computing, Security Issues, Distributed Denial of Service, Defence against DDOS*

1. INTRODUCTION

Today the paradigm is shifting as per the need of the organization as most of them are shifting their databases and applications in cloud and in addition to it they believe on the provider for confidentiality, availability, authentication, and data privacy. These shifting are the result of some features that are provided by these providers such as elasticity, on-demand computing and accessible cloud servicesthereby adding more and more people to shift to this whole new paradigm. Cloud computing is expected to become more popular because of its pay as you go approach, flexibility and reduced maintenance cost in both hardware and software.

Cloud has three service models that include Infrastructure as a model (IaaS), Software as a model(SaaS) and Platform as a model(PaaS). All three functions differently to make cloud exist and work smoothly. SaaS mainly provides users with the ability to use software without even installing them on their PC's or phones. It eliminates the need of operating in your computer as same environment would be provided to you on the cloud interface where you can edit your applications if you want.[1] IaaS on the other hand uses virtual technology to provide physical infrastructure by sharing hardware such as server. These hardware resources are shared with multiple users in one go which makes cloud a multitenant system. Today virtualization is used to increase availability of system along with reducing cost.

Cloud manages a computing resource in a pool which makes it a computing model. Cloud is categorized as public, private and hybrid cloud. Wherein Public cloud is open to everyone who is willing to pay for their usage and in return cloud provider would provide you with storage area and all the resources you need to make business run. [3] Whereas private cloud is a bit different from the later one as in this only addition to the previous one is that private cloud is in full control of a particular organization means you have added security measure in this kind of cloud. Hybrid cloud is the addition of both these cloud public and private where some part belongs to private and some to public. Also Hybrid cloud allows organisations to put in their captiousexercises safe in private cloud along with putting remaining applications in public cloud thereby making it safer.

II. DDoS AND ITS CLASSIFICATION

DDoS attack mainly affects the availability in cloud environment.The attacker mainly degrades the connectivity of the victim's network in the particular domain that includes many other victims. [2] So in DDoS attack attackers first collects many agents and take full control over them and after that by infecting them with malware that responds to their command. After this attacker use these agents to launch the attack in order to deplete the target machine/server. DDoS attacker mainly target to stop the victim's machine to use its resources. In current scenario victim could be a CPU, server or network resources.[6] In cloud environment this can significantly affect the virtual servers to reduce the performance of cloud services.

Today there are varieties of DDoS attacks in the computing world.There are mainly two basic types of DDoS attacks that are bandwidth and resource based attacks. Also both types consume as all the resource and bandwidth of the network being exploited. So based on vulnerability it is divided into

1. Bandwidth depletion attacks:

This form of attack mainly attacks on the bandwidth of the targeted system flood the region of the system from where it validates the requests from users which is done by sending numerous numbers of unwanted illegitimate requests thereby preventing the valid users to reach the system. These are further divided into two parts

i. Flood Attacks:

Flood attacks are initiated by the attackers. In this they, with the help of zombies that are other systems in control of them i.e. done using the botnets created in the home system, use them to post a huge amount of validation request to the attacked system that are invalid which thereby clogs the attacked system and it as a result stops passing valid requests. [3]

ii. Amplification Attacks:

Amplification attacks are based on broadcasting IP addresses to with effect the attacked system. So in amplification attack, first of all attacker sends a large number of IP addresses to a broadcast them to the attacked system either with the help of zombies created by attacking many systems by virus infection or by attacker itself. [2] Again on receiving huge amount of request the attacked server clogs and stops validating valid requests instead gets busy in processing invalid requests sent by the attacker.

1. Resource Depletion Attacks:

Resource depletion attacks are done to somehow disturb the functionality of the destination. During the attack any of the resource can be targeted by the attack. So the successful attack would thus make one or many functionality of the targeted system makes some of its functionality unavailable to valid users. In most cases the target is servers and workstations. This attack not only targets the resources but also target the network resources of the target system. Figure 1 gives you an overview about the attack using DDoS.

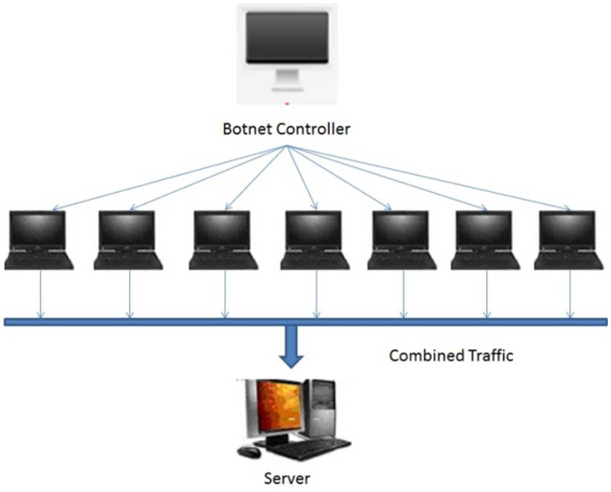

Figure 1

III. DDOS METHODS

1. Detection Methods

Detection process of DDoS attacks is very important in order to give your users an uninterrupted online experience. Early detection of such type of attacks is of at most importance as it accounts for money when you spent lots of time in mitigating DDoS attacks. So as early you start with detection process it allows you to start the mitigation process also [5]. To follow the above stated approach every organization should have at least a separate cell for this purpose of continuously checking whether such attack is approaching them. This helps in better navigation of application and network resources and accounts for larger part of cloud security.

Above we have seen the classification of DDoS attacks that divides it into bandwidth and resource based but attack detection is mainly done at layers mainly application layer and network layer. [4] So in application based detection system we constantly look for any huge traffic that just target to impair the application response by making it highly loaded with incoming requests. Sometimes the attacker sends the application traffic in an encrypted form such as hidden in https traffic. This can be detected by FIPS-140-2 and this mainly accounts for layer 7 attacks.

In network based we experience a huge volume of traffic from user's side to attack the network layer. So in order to negotiate these attempts we take some data from our routers such as the amount of normal traffic we draw from a single user and afterwards use this information to detect whether any user is attempting to attack the network layer by any traffic higher than normal one. [7]

Some IP addresses are more likely to be the attackers during DDoS attacks. Means when any attempt to DDoS attack is put down we got to know about the IP address of the system or the source that triggered it and thus can be used for future detection of such attacks. This can be done by making a collection of such data which can be accessed by the registered and valid users. So in order to get a better cloud security these and many more detection methods must be used to give users more safer experience in cloud operations.

2. Prevention Methods

The cost of recovery after DDoS attack is very high as compared to its prevention because of the fact that this attack may stop your organization stops for a period of time resulting in very high cost to with start it again.[4] So all the organizations that losses much if their website's data is being leaked to someone else are more prone to these attacks. Organizations like e-commerce, healthcare, financial services and all those which mainly run on cloud based software are more prone to DDoS attacks.

Since DDoS can take many forms so these prevention methods should take it in consideration before building defence against them. One of such method could include increasing your bandwidth since DDoS is based on bandwidth the less you would have the easier it would become for the attacker to deplete it. Another important part of your network is your DNS server.[5] The attacker during the attack first tries to breach your server so as to get into your website's resources. Most people get their domains registered along with two servers and think that they have enough layers to beat those attacks but they are wrong since today attacks are launched at a very large scale which can tamper with some limited number of security layers. So an idea of delivering files and documents to your customer via content delivery network would work in such situations.

Another method that can be used is replacing your website's dynamic content with some static content as soon as you get to know about any incoming attack so that attacker has nothing to breach to get access to your network or to your resources. [8]

IV. PROPOSED APPROACH

In order to build this framework which mainly attacks on the server via botnet that controls the other computers connected existing in the same domain as of server, so we need to have our cloud environment setup beforehand that includes some virtual machines, system centre- data protection manager, operation manager, configuration manager, application controller, service manager orchestrator manager, virtual machine manager. All these software helps in creating the cloud environment. Now how this framework works? In earlier methods of DDoS attacks we have seen that first the attacker creates some botnets and then those botnets send malware to computer that are in the same forest domain as of server (in case of cloud environment). Propsed work is figured in Figure 2.

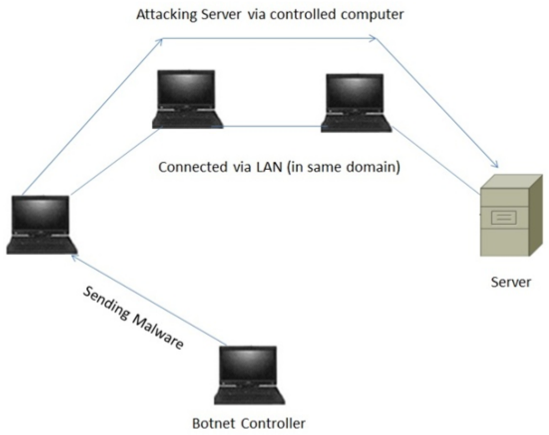
Attacking Server via controlled computer
Connected via LAN (in same domain)
Server
Sending Malware
Botnet Controller

Figure 2

Now because of malware sent to computers in the domain the attacker is able to control them and send enormous amount of request to the server at the same time to make clogged with large number of invalid request so that it doesn't even validate valid users/requests. Now in this case botnets will send in the invalid data from one of the connected computer. So as a result of it now all the requests thrown at the server would first pass through the connected machine either virtual machine or some LAN connected PC'swhich is part of the same domain as of the server. Due to this server may get requests from the same machine with every request having a different IP address thus making it more difficult for the server to understand about the location from where the requests are initiated. This is thus another type of attack which can be instantiated to breach the security wall of the cloud servers that are now somewhat repellent to DDoS attacks.

I. CONCLUSION

DDoSattacks areagrowingproblemwhichhastoend. The obviousquestion isthat“howcan wefindit outthat whetherweare facingtheDDoSattack?” Cloudcomputingprovidesmanybenefitstobothindustrialaswellasothersectorstoo,buttherearemanychallengesincloudcomputing,mainlyin the security are a whereDDoSattack couldmake service unavailable/ unreachable, and there are other methods which I have discussed but most of them give more attention to detecting or track backing or prevention, my new frame work focuses and covers aspect ssuch as different way of attack mainly in cloud environment. The frame work which we haveproposed and discussed here will assist to build as trongarchitecture for security as well as reliable cloud services in the field of cloud computation. And this proposed frame work which enhances these scurity incloud will draw many investors to this core cloud computing concept. Infuturewe should mainly plan to perform as imulation based on the proposed framework above and implement the here stated frame work in cloud environment and constraints such detecting these attacks. Also to detect these types of attacks in different cloud environments such as public, private and hybrid cloud environment.

I. REFERENCES

[1] Detecting DDoS Attack in Cloud Computing Environment, by A.M.Lonea, D.E. Pospescu, H.Tianfield, 2013.

[2] Understanding DDoS attack & its effect in Cloud Computing by Rashmi V.Deshmukh, Kalias K. Devadkar, 2015.

[3] DDoS attack Protection in the Era of Cloud Computing and software defined networking, Bing Wang, Yao Zheng, Wenjing, 2014.

[4] Detecting DDoS attack in Cloud Computing environment using covariance matrix approach, Mohd Nazri Bin Ismail, 2016.

[5] Security issues in cloud computing solution of DDoS and introducing two tier Captcha, Poonam Yadav , Sujata, 2013.

[6] Detect and prevent Denial of service attack in Cloud Computing Environment, R.Udendhran, 2014.

[7] Various techniques of DDoS attacks and its prevention at cloud: a survey, Dalima Parwani, Amit Dutta, piyush Kumar Shukla, Meenu Tahiliyani, 2015.

[8] Data confidentiality, availability and data privacy in cloud computing, Cristof kauba, Stefan mayer, 2013.

[9] DDoS attack using polynomial regression model by Gupta, N and R Guha, 2011.

[10] Intrusion detection in the cloud by Roschke, S. Cheng F and Meinel, 2009.

[11] Cloud computing: Issues and challenges by Dillon, T.C.Wu and E.Chang, 2010.

[12] Securing cloud from DDoS attacks in virtual machine by Bakshi, A and B Yogesh, 2010.

[13] Integrated DDoS attack defense infrastructure for effective attack prevention by Choi, Y.S, 2011.

[14] DDoS defense as a Network Service by Ping Du, Ahmad Salah, 2010.

[15] Cloud computing security management by Sameera Abdularahman Almulla, Chan Yeob Yeun, 2010.