Volume 6, Issue 6, June 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Prevent DDOS Attack in Cloud Using Machine Learning

Anku Jaiswal
M.Tech Student,
SET, Jain University,
Bengaluru, India

Chidananda Murthy P
Assistant Professor,
SET, Jain University,
Bengaluru, India

Madhu BR
Assistant Professor,
SET, Jain University,
Bengaluru, India

Abstract: Cloud computing being one of the most demanding technologies has gained a lot of fame due to various services it provides in the form of utility model. But as we know each technology has both advantages and disadvantages. One of the biggest disadvantages of cloud is security issue. There are many threats to the cloud security and Distributed Denial of Service (DDOS) attack is one of the severe threats. DDOS is a simple but a very powerful attack which makes the resources unavailable to the legitimate client. It is very hard to prevent this type of attack because of different types in which hacker may attack. Distinguishing between malicious and legitimate traffic is a tedious work and also manually filtering the traffic is not possible because of large number of hosts. Resource exhaustion is one of the most common attacks seen today and one of the best techniques would be to build intelligence to the machine so that it could proactively make decision and distinguish between good and bad traffic automatically. This is possible with machine learning techniques. In this paper we have discussed how machine learning can help us to prevent DDOS attack.

Keywords: Cloud Computing, DDOS attack, Machine Learning, Artificial Intelligence

I. INTRODUCTION

With increase in usage of cloud computing to provide the computing resources on demand over the internet, so is the need to secure the computing resources to provide the reliable and secure services to its user by maintaining the confidentiality, integrity and authenticity constraints. Since cloud uses the internet to provide the services, it has become much vulnerable for the various types of attack. One of the major attack issues faced by the cloud platform is DDOS attack. It is a special type of DOS attack in which attacker uses the network of infected computers which are actually bots to exhaust the resources of the target system. The DDOS attack can be mainly classified in to two categories: Bandwidth depletion and resource depletion. The attacks such as UDP and ICMP come under bandwidth depletion and the attack such as TCP sync and IP flood attack comes under resource depletion. It is one of the very notorious types of attack which can make the service unavailable to the legitimate user for very long time hampering the credibility and reliability of the cloud service providers. Most of the defense techniques developed so far has focused on monitoring the network layers to prevent the attack, but the attacker has now shifted their concentration to the application layer since it performs more number of computations per packet so the probability of resource exhaustion increases in this layers.

II. RELATED WORK

Cloud computing one of the most used technologies is still in its stage of development as it suffers different types of security issues. Hence the trust between the client and provider is compromised. To solve these issues a number of solutions based on cryptography, data portioning, multi agent and machine learning can be proposed. [1].According to a survey, 1200 approx. DDOS attack occurs daily. Thousands of DDOS attack can be classified on the basis of Bandwidth depletion and resource depletion. There are various attacks such as Flood attack, Amplification attack, TCP SYN attack. One of the solution to these attack is collaborative use of various solutions such as Firewall, Intrusion detection, Content Filtering and VPN (Virtual Private Networks)[2]. The impact of flooding DDOS attack in cloud can be analyzed by using cloudsim.

This can be done by simulating DDOS attack on the VM instances under Eucalyptus and hence the computational time of VM under attack can be observed [3]. DDOS attack is a very powerful and notorious attack to cloud computing. Defending against this attack is not an easy task as the attacker may use different way to affect the system. Differentiating legitimate an d illegitimate traffic is a tedious task and hence preventing the attack due to various factors such as: Multiple source, filter placement, throughput. Hence automatic defense technique using machine learning technique can be proposed to explore the potential of Artificial Neural Network which helps in preventing DDOS attack [4]. Although a large number of defense techniques has been proposed, preventing DDOS attack is a tough task because today most of the defense techniques rely on human analysts to differentiate between legitimate and illegitimate traffic. Many human relying techniques such as Signature detection , anomaly detection takes up to hours and has many flaws which makes the attack detection a tedious task . Machine learning techniques can be used to make autonomous IDS techniques to prevent DDOS attack [5].Support vector machine is one of the most common method used in machine learning techniques. In this method a training example is taken and by using SVM a model can be used to predict whether the new example falls into the category. Hence new types nonlinear problems can be solved by using SVM [6].Decision tree is another type of machine learning algorithm which uses previous data sets to find new type of data set. Decision tree can be used in intrusion detection system. One of the advantage of this algorithm is it works well with huge data set. Decision tree can be used to find new types of attacks [7].Different types of Machine learning techniques are used to find the detection of DDOS attack. But each technique has its own advantages and disadvantages. Hence various techniques are compared and studied to find an effective Intrusion Detection System [8].

III. DDOS ATTACK

In distributed denial of service attacks, the attackers uses the multiple system to flood the resources and bandwidth of the web server or any target systems, to make the services or resources provided by them unavailable for indefinite time or temporarily for the intended users. The attacks are mainly generated by the multiple system compromised by the botnet to flood the target system. DDOS attack composed of four elements mainly:

- The attack is initiated by the real attacker.
- All the compromised hosts which have bots running on them are controlled by the Master.
- All the packets which results in flooding of the target resources are generated by the zombies.
- The target system mainly web servers are the victims.

Attackers are always one step ahead the detector. A lot of tool has been developed to solve the problem of network layer. Hence the hackers are shifting from network layer to application layer and their main aim is resource exhaustion as it requires less traffic.

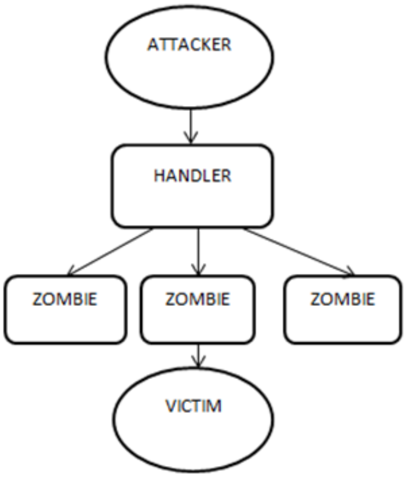

Figure 1: DDOS attack architecture

A. Types of DDOS Attack

Table I Types of DDOS

NAME	DESCRIPTION
Smurf Attack	This attack work with flooding the victim’s bandwidth.
Ping Flood and Ping of Death	This attack is similar to smurf attack but the victim is flooded with thousands of ping packet.
TCP SYN flood	This attack aims at exploiting the server CPU memory.
UDP flood	In this attack UDP packets are flooded against server.
HTTP Flood Attacks	Http floods, which enable attackers to POST large amounts of data to applications
Teardrop attack	This attack utilized vulnerability in the earlier Microsoft Operating Systems and some older versions of Linux whereby improperly framed or overlapping IP fragments were sent to the victim thereby crashing it
Infrastructure attacks	Infrastructure attacks target the Internet’s infrastructure Such as the DNS root servers. They can be extremely dangerous as they have the Potential to bring down the entire Internet.

B. Recent Technique And Their Disadvantages

Table III Techniques and Disadvantages

NAME	DEFINITION	DISADVANTAGE
Blackholing	the process of a service provider blocking all illegitimate traffic and sending the diverted traffic to a “black hole” where it is discarded.	Legitimate packets are discarded along with malicious attack traffic.
Routers	use access control lists (ACLs) to filter out	DDOS attacks generally use valid protocols that are

	"undesirable" traffic, defend against DDOS attacks	essential for an Internet presence, rendering protocol filtering a less effective defence
Firewalls	Blocks certain sites	They are not purpose-built DDOS prevention devices lack of anomaly detection location
IDS	excellent application layer attack-detection capabilities	They cannot detect DDOS attacks using valid packets—and most of today's attacks use valid packets
Signature detection	involves searching network traffic for a series of bytes or packet sequences known to be malicious	They only detect known attacks, a signature must be created for every attack, and novel attacks cannot be detected.
Anomaly detection	The anomaly detection technique centres on the concept of a baseline for network behaviour. This baseline is a description of accepted network behaviour, which is learned or specified by the network administrators, or both.	Disadvantage of anomaly-detection engines is the difficultly of defining rules.

IV. DIFFICULTIES IN PREVENTING DDOS ATTACK

Sites don't know where the attacks are coming from

- Firewalls aren't designed to handle DDOS attacks
- The defense can't be mounted on the hosting provider's infrastructure
- The tools are much more dynamic now. Humans and human processes are not fast enough to keep up with the change.
- It is very difficult to determine the origin of the attack.
- Since the attacks are generated from multiple sources it is very diificult to prevent the attack.

V. MACHINE LEARNING

Machine learning is a type of artificial intelligence (AI) that provides computers with the ability to learn without being explicitly programmed. Machine learning focuses on the development of computer programs that can teach themselves to grow and change when exposed to new data.

Machine learning techniques have ability to implement a system that can learn from data. For example, a machine learning system could be trained on incoming packets to learn to distinguish between intrusive and normal packet. After learning, it can then be used to classify new incoming packets into intrusive and normal packets.

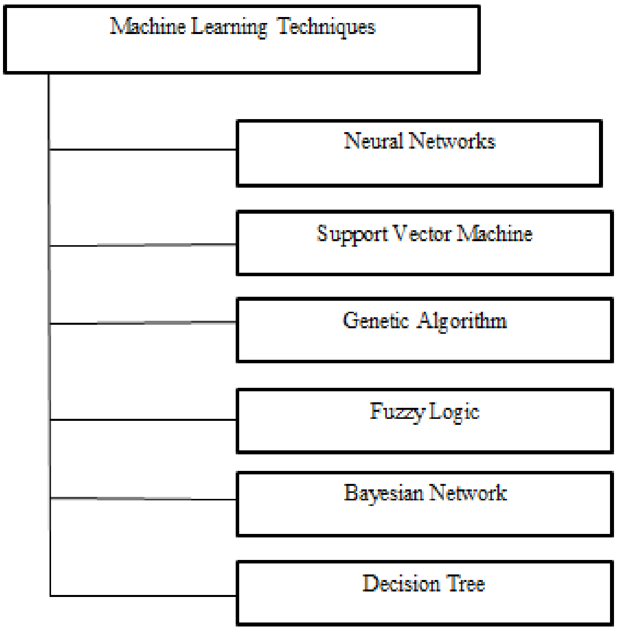

Fig 2: Classification of Machine Learning

A. Artificial neural network

The artificial neural network(ANN) draws its inspiration from the biological neural network which can be used to estimate the given fuction from the given unknown inputs. As the human brain, the ANN is too composed of multiple nodes and connected by the link and each link is associated with some weight value, each nodes take the input and produces the output, which is again passed as the input to the other nodes.

The ANN can be used to determine the complex relationship and pattern between the input data and is considered very effective data modeling tool.

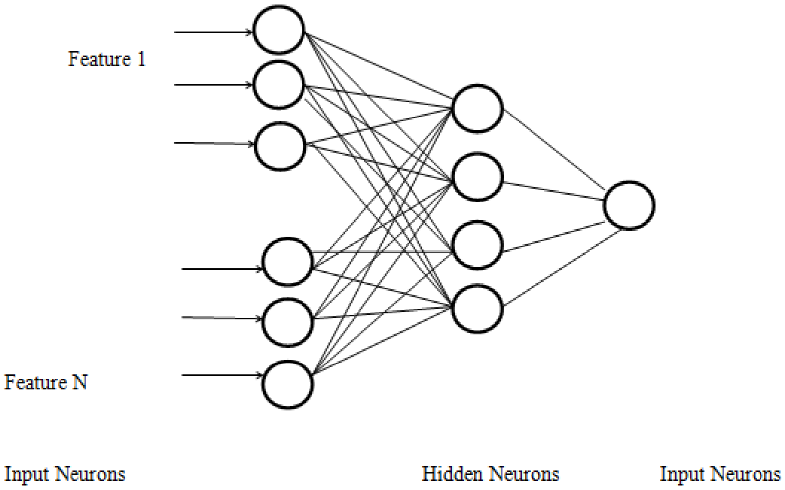

Fig 3: Artificial Neural Network

VI. DDOS PREVENTION APPROACHES

According to [4], machine learning[9][10] can be used to prevent DDOS attack in an automated fashion. Our proposed system has following features:

- Fully automated system to prevent DDOS attack.
- Focus on resource utilization rather than packet monitoring.
- Using Artificial Neural Network for attack detection and storing its result in sample database for future reference.

The proposed system consists of following steps:

- A load monitoring node which continuously monitor the system resources (CPU, NETWORK). If the utilized resource is more than the given threshold value, the incoming packets is identified as anomalous.
- A traffic monitoring node which continuously monitor the packets from different network layers. As packets from different layers are analyzed, so we have sufficient amount of data to analyze whether the request is legitimate or illegitimate.
- Now the server which is the central component of the system, it performs two basic tasks: it receives data from the traffic and load monitoring system and stores it for further processing. Secondly, it continuously monitors the system. If the system is found to be operating in normal condition then baseline profile for these request is maintained and if the system is found under the attack then the feature extracted from the load and traffic monitoring system is store into the Sample Database.

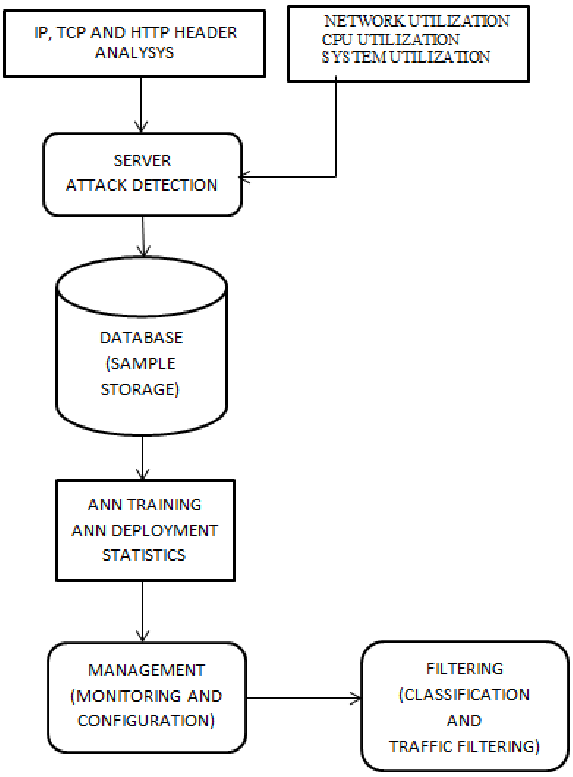

Fig 4: Architecture of the system using neural network

- Database stores the baseline profile data and the data extracted by load and traffic monitoring systems which is used as input for training algorithm.
- Now ANN uses the baseline profile data to train the algorithm and distinguish the difference between the normal packet and the malicious packet which can be used to prevent the attack.
- The filtering node uses the algorithm produced by ANN to filter and drop the malicious packets.
- The monitoring node is basically a web application which helps the management to continuously manage the state of the system.

VII. CONCLUSION

DDOS attack detection is a very complex and complicated problem for cloud computing technology. Despite of using various techniques, DDOS attack is one of the most vulnerable attack .Machine learning based on artificial neural network can be used to achieve excellent solution as it uses automated system. Rather than analyzing network traffic, main aim of this technique is to monitor resources which make it an efficient technique.

VIII. FUTURE WORK

DDOS attack has become major security issue for the cloud computing platform. A lot of research work is required to make the system more secure and provide the trusted and reliable services to its user. Since the system is under the continuous attack, the existing security measures can be improved with the machine learning technique for automated security system, so that very little human intervention is required for monitoring, detecting and preventing the attack.

REFERENCES

[1] Y. Ghebghoub, S. Oukid, and O. Boussaid; "A Survey on Security Issues and the Existing Solutions in Cloud Computing", International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013

[2] Raj Kumar P. Arun,S. Selvakumar; "Distributed Denial of service threat in collaborative environment- A survey on DDOS tools and Traceback mechanism", IEEE International Advance Computing Conference,2009

[3] Mr S.Karthik, Prof J.J.Shah; "Analysis of Simulation of DDOS Attack in Cloud" , Information Communication and Embedded Systems (ICICES), 2014 International Conference

[4] Stefan Seufert and Darragh O'Brien ,"Machine Learning for Automatic Defence against Distributed Denial of Service Attacks", ICC 2007 proceedings.

[5] Chris Sinclair, Lyn Pierce, Sara Matzner "An Application of Machine Learning to Network Intrusion Detection". Phoenix, AZ 06 Dec 1999-10 Dec 1999

[6] J. Burges, "A tutorial on support vector machines for pattern recognition", Data Mining and Knowledge Discovery, vol. 2, pp. 12 1- 167, 1998.

[7] Kamarularifin Abd Jalil, Muhammad Hilmi Kamarudin, Mohamad Noorman Masrek; "Comparison of Machine Learning Algorithms Performance in Detecting Network Intrusion", 2010 International Conference on Networking and Information Technology

[8] Jayveer Singh , Manisha J. Nene , "A Survey on Machine Learning Techniques for Intrusion Detection Systems" , International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013

[9] Sujay Apale, Rupesh Kamble, Manoj Ghodekar, Hitesh Nemade, Rina Waghmode; "Defense Mechanism For Ddos Attack Through Machine Learning", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308

[10] Sergio Armando Guti´errez, John Willian Branch Grupo GIDIA, "Application of Machine Learning Techniques to Distributed Denial of Service (DDoS) Attack Detection: A Systematic Literature Review"