International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 6 258 – 261

An Integrated Approach for detecting DDoS attacks in Cloud Computing

Sarat Akasapu
Department of Computer Science and Engineering
MVGR College of Engineering
Vizianagaram, Andhra Pradesh
saratakasapu@gmail.com

Abstract— With the recent advancement of Cloud Computing, it provides various services for both organizational and individual users such as shared computing resources, storage, networking etc on demand. Even though it offers various benefits to the users still it remains exposed to many types of attacks which attract cyber criminals. The most common type of attacks on Cloud computing is Distributed Denial of Service (DDoS) Attack. DDoS attack is an attack which makes resources unavailable to the user by compromising large number of systems called bots. The attacker infects various systems in order to carry the attack called Botnet.

This thesis aims to implement detection of DDoS attacks through Feature based selection algorithms. For this NSL KDD dataset is used which is a benchmark for Network Intrusion and Detection systems. Feature Selection also called Variable selection or Attribute selection is the method of choosing a subset of significant features for constructing a model. NSL KDD consists of 41 features and categorised as either normal or attack. The attacks are divided into 4 categories: DoS, Probe, U2R and R2L. We divide the dataset into training set and testing datasets by applying 10 fold cross validation. Based on the results we apply classification algorithms such as Decision trees, Random Forest, KNN classification, Naïve Bayes classifier etc and evaluate its accuracy. We can then evaluate which algorithm is better and how it can be better compared to other algorithms.

Keywords – *Cloud Computing, DDoS attack, NSL KDD, Classification algorithm*

*****

I. INTRODUCTION

Cloud Computing is a technology which refers to the provision of hosted services over the Internet. There are three types of cloud models: public cloud, private cloud and hybrid cloud. Public Cloud is cloud infrastructure where the services are offered to the end users for free. Private Cloud is solely operated by a single organization whether managed individually or by third party. Hybrid Cloud consists of some combination of private, public and community cloud services, from different service providers. There are 3 main service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). With Software as a Service you can run applications which you want to use like SharePoint, Office 365 etc. Platform as a Service provides a platform for users in cloud environment in which they can develop, run and execute applications. Infrastructure as a Service provides virtualized environment for users to manage different services like data centres, networking equipment and storage.

As Cloud computing provides many benefits to the users, it has attracted many cyber attackers to exploit the vulnerabilities in it. DDoS attack is the most common attack which targets cloud computing. DDoS attack is a kind of attack where unauthorised person tries to compromise a single system by affecting various systems to target the attack. The intermediate systems which are affected are called Zombies and the main systems are called Handlers. Current defense techniques can only detect malicious packets based on Signature based or Anomaly based technique. To overcome these limitations, Feature based selection methods have been proposed. Feature selection is pre-processing phase before classification which identifies important features of dataset thereby improving prediction accuracy. Feature selection methods can be divided into wrapper, filter and embedded approaches. Filter methods select variables regardless of classification model. Wrapper methods evaluate subset of variables to detect the possible interaction between variables. Embedded method is the combination of both wrapper and filter methods.

II. THEORITICAL BACKGROUND

Denial of Service is an attack which attempts to prevent network resources unavailable to its intended users by temporarily or permanently disrupting services connected to the host. It is accomplished by flooding the victim with massive number of requests and overloading it with fake or illegitimate systems so that the victim cannot handle the request from being fulfilled. Distributed Denial of Service

(DDoS) attack is a DoS attack where various systems flood the bandwidth or resources of targeted system so as to make it more powerful and successful.

Types of DoS Attacks:

Probing Attack

Probing Attack is an attack which is used to collect information about network resources for the sake of bypassing its security controls. Some of the probing attacks are given below.

Ipsweep: An Ipsweep attack is an attack which is used to find which hosts are listening on a network to find vulnerabilities and loop holes in it.

Portsweep: A Portsweep attack attempts to find what are the open ports available in a machine on a network.

Nmap: Nmap is a network mapping tool which performs different scanning techniques like SYN, FIN, ACK etc to find which ports are open and which are closed on a network.

Satan: Satan is a tool designed to probe a computer system for security loopholes. Satan stands for Security Administrator Tool for Analyzing Networks.

Remote to Local (R2L) Attack

Remote to Local attack is an attack where intruder send packets to a system over network that is not having an account on that system but seeks to exploit vulnerability to gain local access of user on that machine.

Imap: Imap attack occurs when an attacker exploits vulnerability in input validation on IMAP server to execute commands on the server.

Ftp_write: Ftp_write attack occurs when an attacker takes advantage of common anonymous ftp misconfiguration.

Phf: Phf attack occurs when a poorly written CGI script try to run commands with privilege level of http server.

Guess_password: Guess_password attack is an attack on guest accounts with no password or easy to guess password.

Netcat: Netcat attack occurs when the attacker uses a Trojan to install and execute netcat program on target system on a specific port.

Warezmaster: Warezmaster exploits a weakness associated with FTP server. This attack occurs when FTP server wrongly, gives write permission to users on the system.

Warezclient: This attack can be initiated after warezmaster attack is executed. Users download illegal warez software after successful warezmaster attack.

User to Root (U2R) attack

User to Root attack occurs when the intruder starts as normal user and gains access to root account by exploiting some vulnerability.

Buffer overflow: Buffer overflow is a vulnerability in which the attacker overwrites the buffer with his own code thereby launching the attack. Some functions in C which are vulnerable to this attack are strcpy(), strcat() , sprintf().

Loadmodule: Loadmodule attack is an attack on SunOS 4.1 systems that use the xnews windows system. Because of the exploit in loadmodule program unauthorized users can gain root access on the local machine.

Perl Attack: Perl attack exploits a flaw in some Perl implementations. Suidperl is a version of perl that supports saved set user ID and set group ID scripts. An attacker may compromise the system using those scripts and gain access.

Ntfsdos attack: It is a console based attack which restarts the system from a floppy disk containing NTFSDOS.EXE.

Rootkit: Rootkit is a collection of software tools that enable attacker to gain administrative access to a computer. A hacker usually installs a rootkit on a victim machine after gaining user level access, either by bypassing a known weakness in the system or cracking a password.

DoS attack types

Land Attack: Land attack is an attack where an intruder sends a forged SYN packet where source address and destination address are same.

Ping of Death: Ping of Death attack occurs when an attacker intentionally sends an IP packet with size greater than 65,536 bytes allowed by the IP protocol.

Smurf Attack: Smurf attack occurs when the intruder sends ICMP echo request packets to IP broadcast addresses from another machine to create denial of service attack.

Teardrop attack: Teardrop attack is an attack where attacker sends broken packets to a victim system. Since the target system cannot rearrange them, the packets overlap one another crashing it.

Neptune Attack: Neptune attack occurs when a huge number of SYN packets are sent to target system using forged IP address.

 ISSN: 2321-8169
258 – 261

III. FLOW DIAGRAM

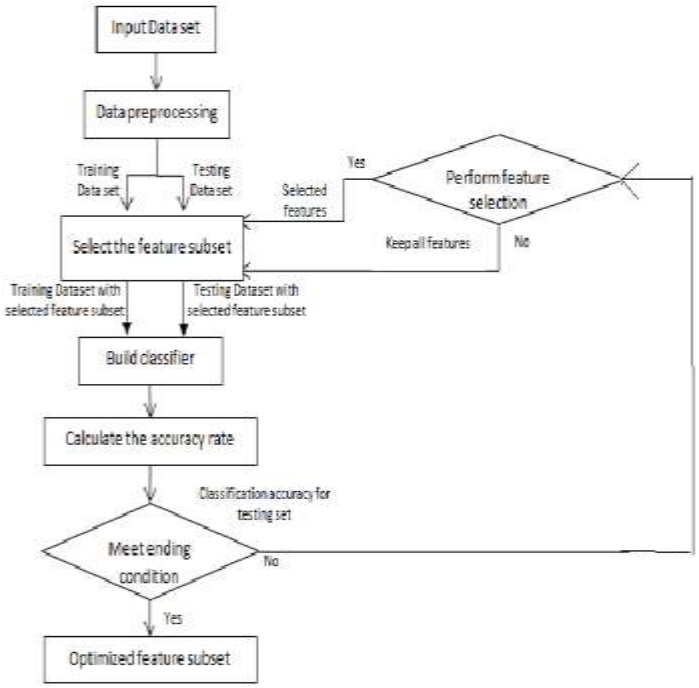

Figure.1*Procedure for feature selection*

The diagram shows the procedure to select best subset from the given input dataset. First the dataset is given as in input and preprocessing is done on that. Then the dataset is divided into training and testing dataset. Perform feature selection by selecting relevant features. Then apply classifier for classification. Calculate the accuracy rate for the applied classifier and select the best subset from it.

IV. IMPLEMENTATION AND ANALYSIS

For implemention we use RStudio. Rstudio is a free and open source Integrated Development Environment (IDE) for statistical computing and graphics. It is written in Java and C++. It runs on Windows, macOS and Linux.

Following are the steps for implementing classification algorithm.

1. Download the RStudio setup from its official site.
2. Load the dataset into R.
3. Load required libraries which are necessary for implementation.
4. Perform Cross validation for the given dataset.
5. Apply classification algorithms using ‘fit’ function.
6. Compare the accuracy of different algorithms.
7. Plot the results.

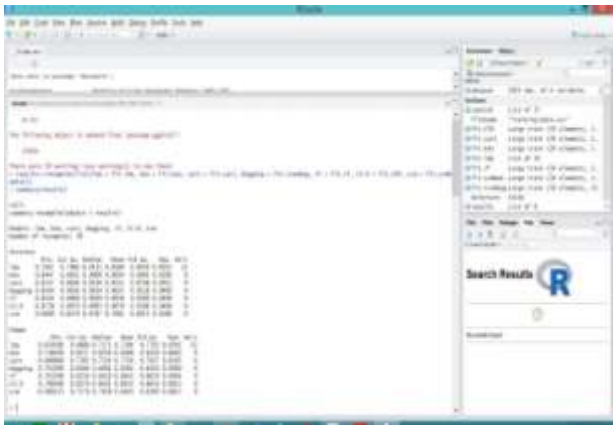

Figure.2*Accuracy Comparision*

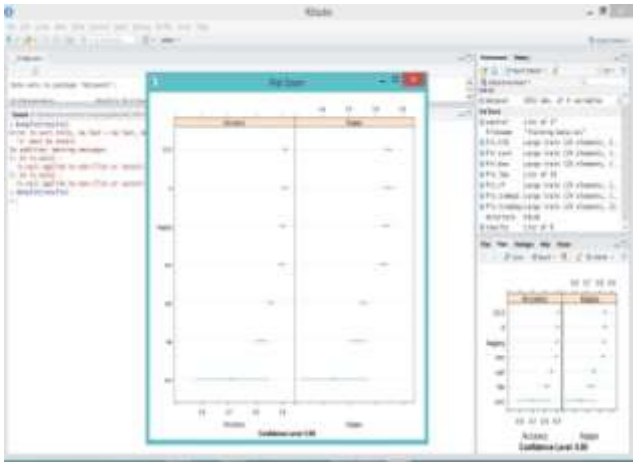

Figure.3*Dotplot of algorithms*

V. CONCLUSION AND FUTURE SCOPE

Machine learning has become an important domain in many fields. In this project we took NSL KDD dataset that is benchmark for Network Intrusion and Detection and applied different classification algorithms by using Feature based selection methods. We compared the accuracy metric and kappa metric of each algorithm and find which classifier gives best accuracy.

In this we applied existing popular algorithms in machine learning and generated results. In future we can use emerging and new algorithms on different datasets in Cloud and implement them. Also we can set up a public or private cloud and try to implement the datasets that are present in them.

REFERENCES

[1] Opeyemi Osanaiye, Haibin Cai, Kim-Kwang Raymond Choo, Ali Dehghantanha, Zheng Xu and Mqhele Dlodlo “Ensemble based Multi Filter Feature Selection method for DDoS detection in Cloud Computing” EURASIP Journal on Wireless Communications and Networking, 2016

[2] Preeti Aggrawal, Sudhir Kumar Sharma "Analysis of KDD Dataset Attributes – Class wise for Intrusion Detection" Science Direct 2015, pp.842-851.

[3] Mohammed A. Ambusaidi, Xiangjian He, Priyadarsi Nanda, Zhiyuan Tan "Building an IDS using filter-based feature selection algorithm" IEEE Transactions on Computers, Vol.,No., November 2014.

[4] Hee-su Chae, Sang Hyun Choi "Feature Selection for efficient Intrusion Detection using Attribute Ratio" International Journal of Computers and Communications, Vol 8, 2014

[5] Md. Al Mehedi Hasan, Mohammed Nasser, Shamim Ahmad, Khademul Islam Molla "Feature Selection for Intrusion Detection using Random Forest" Journal of Information Security 2016, pp.129-140

[6] Opeyemi.A. Osanaiye "IP Spoofing Detection for preventing DDoS Attack in Cloud Computing" International Conference on Intelligence in Next Generation Networks 2015

[7] Opeyemi A. Osanaiye "TCP/IP Header classification for detecting Spoofed DDoS attack in Cloud environment" 16th International Conference on Computer as a Tool 2015, pp. 1-6

[8] Khorshed, Md Tanzim, ABM Shawkat Ali, and Saleh A. Wasimi. "A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing." Future Generation computer systems 28.6 (2012): 833-851.

[9] Wang, Bing, et al. "DDoS attack protection in the era of cloud computing and software-defined networking." Computer Networks 81 (2015): 308-319.

[10] Lonea, Alina Madalina, Daniela Elena Popescu, and Huanglory Tianfield. "Detecting DDoS attacks in cloud computing environment." International Journal of Computers Communications & Control 8.1 (2013): 70-78.

[11] Choi, Junho, et al. "Detecting web based DDoS attack using MapReduce operations in cloud computing environment." Journal of internet services and information security 3.3/4 (2013): 28-37.

[12] Yan, Qiao, and F. Richard Yu. "Distributed denial of service attacks in software-defined networking with cloud computing." IEEE Communications Magazine 53.4 (2015): 52-59.

[13] Xiao, Zhifeng, and Yang Xiao. "Security and privacy in cloud computing." IEEE Communications Surveys & Tutorials 15.2 (2013): 843-859.

[14] Karnwal, Tarun, T. Sivakumar, and G. Aghila. "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack." Electrical, Electronics and Computer Science (SCEECS), 2012 IEEE Students' Conference on. IEEE, 2012.

[15] Lombardi, Flavio, and Roberto Di Pietro. "Secure virtualization for cloud computing." Journal of Network and Computer Applications 34.4 (2011): 1113-1122.

[16] Deshmukh, Rashmi V., and Kailas K. Devadkar. "Understanding DDoS attack & its effect in cloud environment." Procedia Computer Science 49 (2015): 202-210.

[17] Chonka, Ashley, and Jemal Abawajy. "Detecting and mitigating HX-DoS attacks against cloud web services." Network-Based Information Systems (NBiS), 2012 15th International Conference on. IEEE, 2012.