[NC-Rase 18]
DOI: 10.5281/zenodo.1485443

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

DESIGN EFFICIENT ANTI DDOS INTRUSION DETECTION SYSTEM FOR CLOUDCOMPUTING

Miss Khot Meghmala Balwant & Dr. S. D. Bhoite
Research Scholar, Chhatrapati Shahu Institute of Business Education and Research, India
Associate Professor, Chhatrapati Shahu Institute of Business Education and Research, India

ABSTRACT

Today small and medium companies are increasingly realizing that simply by tapping into the Cloud they can gain fast access to best business applications Cloud services are becoming increasingly popular, both among the public and business enterprises. As more organizations are relying on cloud computing technology for their business operations. With more organizations moving onto cloud platforms, there will need to be new types of security best practices to help secure their environments. Data leaks and security breaches can be messy from an IT perspective to design Anti DDOS Solution.

Now a days Denial of Service or Distributed Denial of Service (DDoS) attacks are generally large-scale web based attacks against companies or websites. In this Research paper focus on a practical DDOS defense system that can protect the availability of web services during severe DDOS attacks with the help of Anti DDOS. The proposed system provides multistage detection through various modules like checking source, login test, turing test to fix whether the client is attacker or legitimate client, if detected that particular client address will be blocked, the service could not be provided. So our system protects legitimate traffic from a huge volume of DDOS traffic when an attack occurs. As there is strong need of designing Anti-DDOS IDS and hence the proposed research title is "Design Efficient Anti-DDOS Intrusion Detection System for Cloud Computing".

Keywords: *IDS, Cloud Computing DDOS etc.*

I. INTRODUCTION

In today's ever-changing business climate, it's critical that small business owners get what they need right when they need it. Whether they're on their computers, tablets or mobile phones, it's more important than ever for businesspeople to have information right at their fingertips, wherever they are. This is exactly the convenience that cloud computing provides.

Today small and medium companies are increasingly realizing that simply by tapping into the Cloud they can gain fast access to best business applications.

Cloud services are becoming increasingly popular, both among the public and business enterprises. As more organizations are relying on cloud computing technology for their business operations.

II. OBJECTIVE

The proposed system provide a multistage detection to more precisely detect the possible attackers. So with our Anti-DDoS software model will improve the existing DDoS mitigation technologies

- To study existing security system to mitigate DDOS attacks.
- To design and develop an Anti-DDOS Intrusion Detection System for Cloud Computing to defend from DDOS attacks.

Scope

The proposed Anti DDoS will provide good service to legitimate data exchange during the attack, which is the important goal of DDoS defense. DDoS mitigation also requires identifying incoming traffic to separate human traffic from human-like bots which will be done by the proposed system with attack detection.

III. PROBLEM STATEMENT

Firewall protects the front access points of system and is treated as the first line of defense. Firewalls [8] are used to deny or allow protocols, ports or IP addresses. It diverts incoming traffic according to predefined policy.

Different firewalls used in network for security purpose. As firewalls sniff the network packets at the boundary of a network, insider attacks cannot be detected by traditional firewalls. Few DoS or DDoS attacks are also too complex to detect using traditional firewalls. For instance, if there is an attack on port 80 (web service), firewalls cannot distinguish good traffic from DoS attack traffic

So there limitations of firewalls like:

- Allow/deny packet by inspecting only header information such as source or destination address, port numbers etc.
- Do not detect malicious code in packets.
- Cannot prevent against spoofing and fragment attack.
- Firewalls Cannot Distinguish between Malicious and Legitimate User

As many organizations moving onto cloud platforms and security is the major challenge for acceptance of cloud platform, there will need to be new types of security practices to help secure their environments. One of these security challenges is how to mitigate with DDoS (Distributed Denial-of-Service attack (DDoS attack).DDoS not only cost in terms of serious money but also can affect your business and image in seconds .So there is strong need of designing Anti-DDOS IDS. Cloud computing also suffers from various traditional attacks such as IP spoofing, Address Resolution Protocol spoofing, Routing information Protocol attack, Flooding, Denial of Service (DoS), Distributed Denial of Service (DDoS) etc. So Efficient intrusion detection systems (IDS) and intrusion prevention systems (IPS) should be incorporated in Cloud infrastructure to mitigate these attacks.

IV. BACKGROUND

The Intrusion detection system in a similar way complements the firewall security. The firewall protects an organization from malicious attacks from the Internet and the Intrusion detection system detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security**.** Intrusion detection systems are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for malicious activities or policy violations and produces reports to a management station. An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.

V. TYPES OF DIFFERENT TYPES OF ATTACK

Denial of Service (DoS): In DoS attack, legitimate networking requests are not served because attacker makes the resources either too busy or full to serve the request. Hence the legitimate user cannot access the services of a machine or network resources. Example: apache, mail bomb, back etc.

Probing (Probe): In probing, attacker scans a machine or a network device for gathering the information about weaknesses or vulnerabilities that can be exploited later to compromise the target system. Example: saint, mscan, nmap *etc.*

User to Root (U2R): In U2R attacks, an authorized user attempt to abuse the vulnerabilities of the system in order to gain privilege of root user for which they are not authorized. Example: perl, xterm, Fd-format etc.

ISSN 2348 – 8034
Impact Factor- 5.070

Remote to Local (R2L): In this type of attacks, a remote user tries to gain access as a local user to a local machine by sending packets to a machine over the internet. An external intruder exploits vulnerabilities of the system to access the privileges of a local user. Example: xlock, phf, guest *etc*.

VI. PROPOSED SYSTEM

The proposed work also aims to investigate different issues over IDS. When an intruder attacks a system, the ideal response would be to stop his activity before any damage or access to sensitive information occurs.

Proposed modules

1) Checking source

In this module we are checking the source of attack. We are providing authentication for client for login. If client attacks with some pattern then by identifying that clients IP address, we are finding its source.

2) Counting

In this module we are recording the source address destination address and the time at which client performs login test. After login successful the counting module is reset. It will be enable by the Attack Detection module when there are some suspected traffic been detected.

3) Turing Test Module

So our Turing Test module challenges the suspected client, waits for their answers, and decides if the requesters are humans or programs

4) Question Generation Module

In this module if client fails to perform Login then admin will ask some questions which client has to answer perfectly. The question will be stored by admin at the time of client registration

Proposed architecture

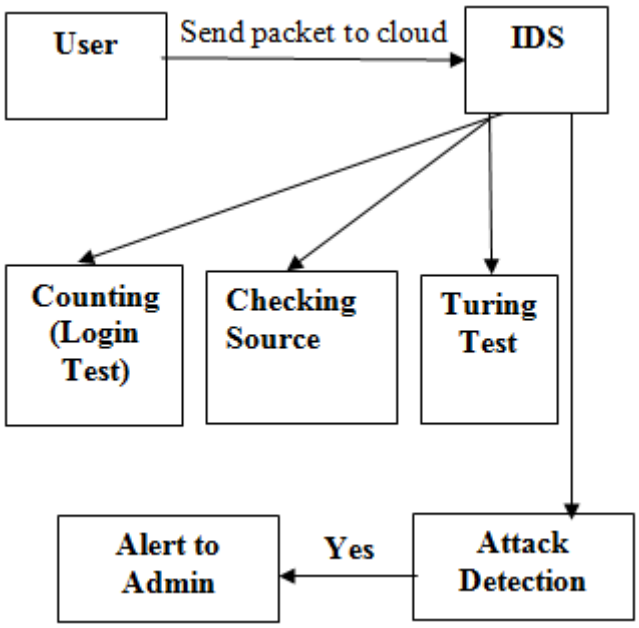

Fig 1. System Architecture

The system architecture of login test,turing test, intrusion detection, percentage of attack display, intrusion response and blocking the suspected client. In case of intrusion detection, it drops attacker packet, then sends alert message about the attack detected. This multistage approach is suitable for preventing Cloud system from DDoS attack.

[NC-Rase 18]
DOI: 10.5281/zenodo.1485443
ISSN 2348 – 8034
Impact Factor- 5.070

Proposed algorithm

Apriori Algorithm

Apriori algorithm is an algorithm for frequent item set mining and association rule learning over transaction databases. It's followed by identifying the frequent individual items in the database and extending them to larger and larger item sets as long as those item sets appear sufficiently often in the database. The frequent item sets determined by Apriori can be used to determine association rules which highlight general trends in the database

C_k: Candidate item set of size k
L_k : Frequent item set of size k
L_1= {frequent items};
For (k=1; L_k!=Φ;k++) do begin
C_{k+1} = candidates generated from L_k;
For each transaction *t* in database do
Increment the count of all candidates in C_{k+1}
Those are contained in *t*
L_{k+1} = candidates in C_{k+1} with min_support
End
Return U_k L_k;

Fig.2: Apriori Candidate Itemset Generation Algorithm

A support value is provided to the algorithm. First, the algorithm generates a list of candidate itemsets, which includes all of the itemsets appearing within the dataset. Of the candidate itemsets generated, an itemset can be determined to be frequent if the number of transactions that it appears in is greater than the support value.

Explicit association rules can then trivially be generated by traversing the frequent itemsets, and computing associated confidence levels. Confidence is the proportion of the transactions containing item A which also contains item B, and is calculated as

$$\text{Confidence}(A \Rightarrow B) = \frac{\text{Support}(A \cup B)}{\text{Support}(A)}$$

ID	Rule	Support	Confidence
r1	{a, b, c}⇒{e}	0.5	1.0
r2	{a}→{c, e, f}	0.5	0.66
r3	{a, b} →{e, f}	0.5	1.0
r4	{b} →{e, f}	0.75	0.75
r5	{a} →{e, f}	0.75	1.0
r6	{c} →{f}	0.5	1.0
r7	{a}→{b}	0.5	0.66
…	…	…	…

ISSN 2348 – 8034
Impact Factor- 5.070

VII. ANALYSIS AND DISCUSION

Experiment

KDD CUP 99

Data mining is the modern technique for analysis of huge of data such as KDD CUP 99 data set that is applied in network intrusion detection. Large amount of data can be handled with the data mining technology. It is still in developing state, it can become more effective as it is growing rapidly. KDD CUP 99 data set in the classification of attacks and compared their results which have been reached, and being used of the performance measurement such as, True Positive Rate (TP), False Alarm Rate(FP), Percentage of Successful Prediction (PSP) and training time (TT) to show the results, the reason for this survey is to compare the results and select the best system for detecting intrusion(classification).

KDD99 was the used data set for most researchers in the development of algorithms to determine the intrusion, which dealt with the data set in different ways and multiple processors to reach the best results.

KDD 99 that contains the Connection classified as normal and attack, into different distributions, while attacks were classified into four sections represented into DoS (deny of service), Probe (information gathering), U2R (user to root), U2L (remote to local) in different numbers

Hardware requirements

The minimum hardware requirements are:

Hard disk	:	500GB and above
RAM	:	4 GB and above
Processor speed	:	i3 and above

Software requirements

The minimum requirements for detection and prevention of phishing attacks are:

Operating System	:	Windows XP/7
Technology Used	:	JSP, Servlet, JDBC
Development IDE	:	Net beans 7.1

Implementation and Results

First we build the application to implement our various modules to tets whether the client is a human being or program. After successful conduction of these modules, we used attack simulation and dataset used for experiment is KDD CUP 99.We successfully implemented attack detection module and finally attack percentage was displayed to user.

VIII. CONCLUSION

Several intrusions which can threat integrity, confidentiality and availability of Cloud services in the future. One of the existing solutions viz. firewall may not be sufficient to solve Cloud security issues. The paper emphasized the usage of alternative options to incorporate multistage intrusion detection or intrusion prevention techniques into Cloud

REFERENCES

1. *Murat Kantarcioglu and Wei Jiang, "Incentive Compatible Privacy-Preserving Data Analysis", IEEE transactions on knowledge and data engineering, vol. 25, no. 6, june 2013.*
2. *Miss Khot Meghmala Balwant, Dr.S.D.Bhoite "A Survey On "A Survey on Design Anti DDOS Intrusion Detection System for cloud computing ", International Journal of Ongoing Research in Science and Engineering (IJORSE)Volume 2 Issue 9 SEP 2018,ISSN 2456-8481*

[NC-Rase 18] ISSN 2348 – 8034
DOI: 10.5281/zenodo.1485443 Impact Factor- 5.070

3. *M. Dhanalak," Effective Incentive Compatible Model for Privacy Preservation of Information in Secure Data Sharing and Publishing" International Journal of Computer Applications (0975 – 8887) Volume 96– No.16, June 2014*
4. *M. Kantarcioglu and C. Clifton, "Privacy-Preserving Distributed Mining of Association Rules on Horizontally Partitioned Data," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 9, pp. 1026-1037, Sept. 2004.*
5. *W. Du and Z. Zhan, "Building Decision Tree Classifier on Private Data," Proc. IEEE Int'l Conf. Data Mining Workshop Privacy, Security, and Data Mining, C.Clifton and V. Estivill-Castro, eds.,vol. 14, pp. 1-8,Dec. 2002.*
6. *J. Vaidya and C. Clifton, "Privacy Preserving*
7. *Association Rule Mining in Vertically Partitioned Data," Proc. ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (SIGKDD '02), pp. 639-644, July 2002.*
8. *R. Agrawal and E. Terzi, "On Honesty in Sovereign Information Sharing," Proc. Int'l Conf. Advances in Database Technology, pp. 240-256, 2006.*
9. *M. Kantarcioglu and R. Nix, "Incentive Compatible Distributed Data Mining," Proc. IEEE Int'l Conf. Soc. Computing/IEEE Int'l Conf. Privacy, Security*
10. *https://en.wikipedia.org/wiki/DDoS_mitigation*
11. *Chirag Modi, Dhiren Patel, Hiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan,"A Survey of Intrusion Detection Techniques in Cloud", Centre for Cyber Security Sciences, City University ,London*
12. *https://blog.radware.com/security/2013/05/can-firewall-and-ips-block-ddos-attacks/*
13. *Marjan Kuchaki Rafsanjania, Zahara Asghari Varzaneha, 2013," Intrusion Detection by Data Mining Algorithms: A Review"*
14. *http://dwgeek.com/mining-frequent-itemsets-apriori-algorithm.html/*