Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 3, pp. 657–666
DOI : 10.47974/JDMSC-1736

Performance analysis of trusted security environment in cloud

Satyajeet Sharma *
Bhavna Sharma †
Department of Computer Science and Engineering
JECRC University
Jaipur
Rajasthan
India

Abstract

This paper is about to elaborating the data mining into intrusion acknowledgment system upgrades the execution has ended up being one of the critical anxieties in interference discovery. The framework is related for portraying log information and perceiving interruptions. With the expanded utilization of multiple computers and direct entry to web, the approaches to manage strike and trap a framework have in addition broadened. The truth is to indicate unmistakable evidence of assaults utilizing IDS structures proposed for the cloud later finishing gathering figuring the log instructive social event to be found. DDoS is one of most loved decision for programmers. There were numerous Intrusion Detection Techniques to distinguish DDoS assault like SNORT, Suricata and so on. In this paper a proposed calculation Packet Count Inspection and Filtering is utilized to distinguish and dispose of satirize bundles by considering transmission postpone time and least, greatest edges which expands reaction time of Intrusion Detection Process in cloud condition with actualizing encryption.

Subject Classification: *Primary 68M25, Secondary 68P25.*

Keywords: *Classifier, Clustering, Data mining, DDoS, Intrusion detection, KDD Dataset, Machine learning.*

1. Introduction

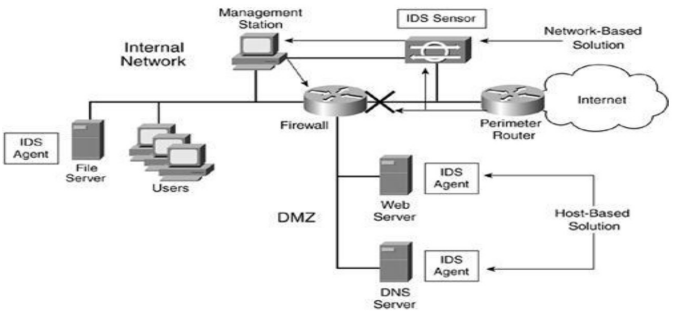
A cloud is a type level contracts set up through conciliation among the master community and buyers.[9]. Distributed computing insinuates

* *E-mail:* **sharma.satyajeet24@gmail.com (Corresponding Author)**
† *E-mail:* **bhavna.sharma@jecrcu.edu.in**

© Taru Publications

together the applications pass on as organizations in wealth of an example of a parallel and distributed structure is a cloud, which is made up of a number of virtualized PCs that are connected to one another and displayed as at least one single pool of resources. [8] As the growth done the firewalls are in nearness to shield these systems from PC threats. While these traditional approaches to manage compose security have focused on evasion, mastermind interference area has ended up being dynamically basic starting late to enable firms to diminish undetected intrusion.[11]

Host-Based IDS can spot attacks that can't be seen by Network based IDS. Host base IDS found in Figure 1 as follows:



(Ref:https://www.researchgate.net/publication/304888649_A_Pattern_Matching_Algorithm_for_Reducing_False_Positive_in_ Signature_Based_Intrusion_Detection_System)

Figure 1

Host Based IDS

Manhandle acknowledgment is stressed over finding interlopers who are attempting to break into a system by abusing some known defenselessness. An intrusion distinguishing proof structure again and again breaks down late development to known interference circumstances to ensure that not less than one attackers are not end evoking to mishandle known vulnerabilities. The imitated attacks come under one of the following four categories: Denial of Service Attack (DoS), User to Root Attack (U2R), Remote to Local Attack, and Cyberattack (R2L).[14]

Here hops count is to be used to indicates the total number of connected network devices used to transfer data from source to destination nodes. Allow any router to adjust a packet's time to live field whenever it gets one (TTL). Any packets with a 0 TTL value that are received here are dropped by the router. In the case of routing problems, this avoids packets from continuously bouncing across the network. The TTL establishes a cap on how many hops a packet may make before being destroyed. As IP

packets are sent, routers alter them by decreasing the corresponding TTL or hop limit parameters. Packets having a resulting field value of 0 or less are not forwarded by routers. This stops packets from becoming stuck in a loop indefinitely.

The integration increases customer trust in the cloud and cloud security as a result of the environment's demand. Many heuristic algorithms have been created and utilized to handle this problem, but identifying the best approach for tackling a specific kind of work assignment problem and discovering a regular update on it. The creation of a system that can identify network intrusion can greatly benefit from data mining. After viewing all previous work, a new concept is to added in the Hop count algorithm for making safe the data packet travelling.[12] Comparative analysis with HCIF algorithms with the new PCIF algorithm indicates that packets are much safer than earlier.

2. Theoretical Background

The purpose of this Literature survey is to include the significance of IDS. Intrusion Detection Systems are dynamically a key bit of structures obstruction. IDS are part into two arrangements: manhandle acknowledgment structures and variation from the norm revelation systems.[7] Diverse techniques have been created to address the insider risk in cloud frameworks. Oversee based ace structures and measurable methodologies have been acclimated to distinguish the interference over cloud frameworks. As watched that greater datasets to apply on IDS turns out to be more dreadful. To deal with these issues groups of data mining methodology displayed.

Rate Denial of Service ambush is an impelled kind of DoS attack which has high disguise characteristics on account of its execution like normal development.[13] On account of these characteristics of LDoS, starting at now existing apparatus and IDS have low adequacy in acknowledgment of LDoS ambushes and in this way these strikes are productive in clumsy true-blue customers from get to the framework resources.[5] By far most of their searchers propose to take off changes in traditions, switch, sort out game-plan, center point functionalities and framework geography in their proposed course of action which is exceptionally outlandish. This paper shows data burrowing-based advance for area of LDoS attack without revealing any upgrades in the framework condition. Test comes to fruition are given to help the proposed system.[2] The examination moreover gives hindrances of each technique to choose on the off chance that they do or do

not meet the security requirements of the distributed figuring condition. We also cover the IDS process, which employs multiple acknowledgement mechanisms to handle cloud security concerns. [3]The IDS with get-together is shown for the relentless unquestionable affirmation of strikes to complete high accuracy and recognizing confirmation rate and in addition low false alert rate.[4]

3. Methodology

Standard Hop Count Filtering Algorithm which is used to distinguish derided and honest to goodness groups is according to the accompanying: Standard Hop Count Filtering Algorithm is utilized to identify spoofed and authentic packets.

System Architecture

The administrator might track network activity by installing HIDS on the host system. However, there would be performance problems such as overloading of the hosting IDS and data packet loss with the quick flow of big volume data as in the cloud model. The host's HIDS would also be deactivated if it were to come under an offensive attack. In these circumstances, the recommended procedure should be used to pass the packet, which will thereafter be discarded in accordance with the regulations.

Algorithm Design

DoS attacks frequently target a large number of hosts;thus, we must consider the scenario in which there are several active flooding sources. A total of F packets is flooded by n flooding sources, each of which

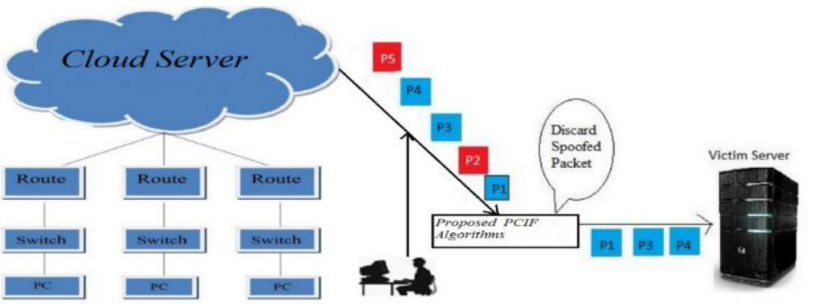


Figure 2

System Architecture Flow

generates Fn faked packets. Figure 2 shows the hop-count distribution of spoof packets sent from two flooding sources. Every flooding source, it has been found, generates traffic with a unique, recognizable hop-count value. The false source I packets that HCF can identify are represented by Fn 1 I, where h_i is the number of hops between the flooded source I and the victims. According to n flooding sources, Z% of faked packets may be such

$$Z = \frac{\frac{F}{n}(1-\alpha_{h_1}) + \ldots + \frac{F}{n}(1-\alpha_{h_n})}{F}$$

$$= 1 - \frac{1}{n}\sum_{i=1}^{n}\alpha_{h_i}$$

According to this equation, having numerous flooding sources results in an overall effectiveness that falls somewhere between the most effective source I with the greatest hi and the least effective source (j) with the smallest hj. The HCF's capacity to recognize spoof IP packets is unaffected by the addition of additional flooding sources. Contrarily, because the hop-count distribution is Gaussian, the filter is able to detect and eliminate more faked IP packets when there are several flooding sources present compared to when there is just one flooding source.

To address the center issue of an interruption discovery framework (IDS), the precision of the identification comes about, in this proposal as in Figure 3

To address the core problem of an intrusion detection system (IDS), the exactness of the detection results, in this thesis, a Packet Count Inspection and Filtering Algorithm for Network Intrusion exposures that possess highly accurate intrusion detection capability such as:

- It first describes the information set used and IDS architecture, followed by a detailed description of the IDS components.
- The dataset used for the evaluation is described for all assed data set in form of packet
- Describes an intrusion-tolerant mechanism improves the reliability of the IDS since it prevents discontinuity in the detection service.
- An new algorithm based on the Hop Count Filtering approach is to design which analyzing through the program activities in intrusion detection as a experiments.
- The random data sets are icked to export results

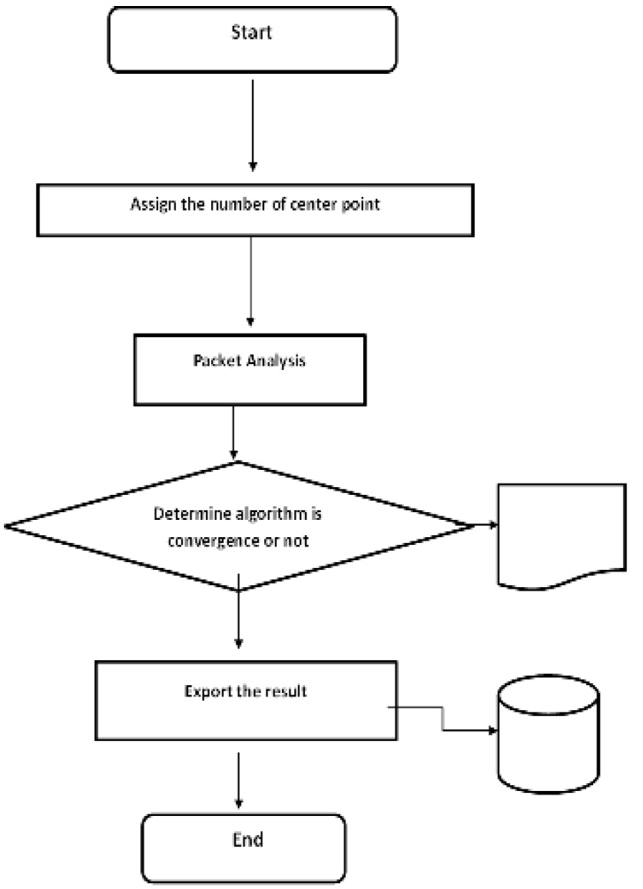


Figure 3

Process Flow of Proposed Approach

- As a result it seen that this approach is able to effectively detect intrusive program behavior.

Functional Work

New Algorithm is design after learning of earlier work and found the new key value to be inserted in the packet to safe it. For changing in the concept of delay time the used formula is taken as

N = no. of links = no. of hops = no. of routers +1 = 3

File size = L bits

Bandwidth = R bps

Propagation speed = t meter/sec
Distance = d meters
Transmission delay = (N*L)/R = (3*L)/R sec
Propagation delay = N*(d/t) = (3*d)/t sec
Total time = 3*(L/R + d/t) sec

Algorithm (n, λ, μ, TTLmax, TTLi)

1. Iteration of each packet i=1 to random
2. Pick the packet and check with own stored authorized packet value
Ti = 3*(L/R + d/t)
3. if ((Ti>Tmax)
"Packet to be Discard"
4. Else if (Ti<=Tmin))
Hi=TTLmax-TTLi
5. else
Hi=TTLmax-Ti
hit1 (itr,i)=Hi
while Hi>30
Hi=Hi-30
6. End If
7. If ((Hi==0)&&(Hi==30))
"Packet to be Drop"
8. Else if (Hi==Hstored)
"Packet Legitimate"
9. Else
"Need to Spoofed Packet"
10. End If
11. End If
12. End For

4. Result

In this out comes is to separate the packets flow in the network system that is to effective result. When HS is not encrypted it was not able to discriminate the discard and dropout packets as no hop count was falling in that range may be corrected due to hacking. According to Figure 4 after encryption no one can get actual hop stored table so clear picture of all four possibility is appearing.

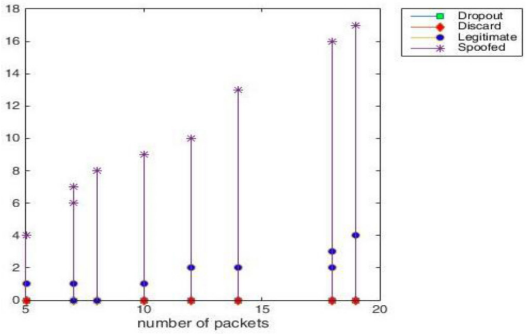


Figure 4

Bifurcate the packets in cloud

In this result is show that it is to be flow of 100 packet and calculate delay of every packet When no, of packets is 100-time delay of each packet is shown in Figure 5 graph. I this figure packets 100 packets are specify the time delay which is in randomize manner.

When no, of packets is 100 hop count of each packet is shown in Figure 6

In this result is show that is to be hop count this hop count start from 0 to 30. According to the resulted and comparison between HCIF and PCIF it found that the PCIF is much better in respect to performance and safety. The PCIF specify the hiding of packet from spoofer by putting the key value which is encrypted through program.Also, this key value is Program dependent which can be manipulated in real word as per need.

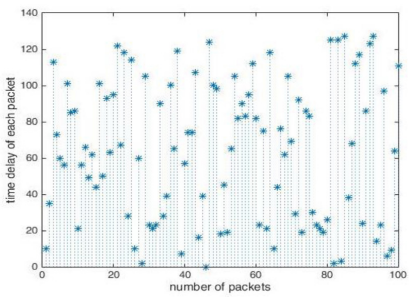


Figure 5

100 Time Delay output

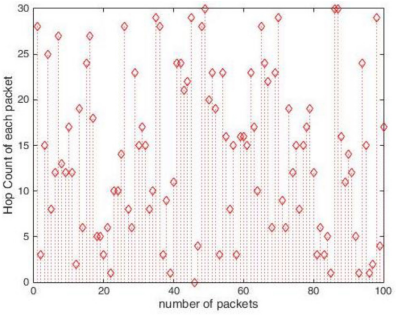


Figure 6

100 Hop count output

5. Discussion and Conclusion

In this work a new Packet Count Inspection and filtering (PCIF) method is proposed to overcome the issue of hacker reorganization of packet. In this the packet delivery is encrypted by a key value so that generated delivery to inferred and spoofed IP packets. This work is extending the work of Hop Count Inspection and Filtering (HCIF) method. The designing of PCIF filtering function follows the implementation of a special key set to discriminations of actual packets from the spoofed packets. This new approach is capable of identifying the DDoS attacks and its deviations on early stages of data transfers. After applying the new key set hence reduces the probability of losses and attacks occurrences on IDS. The approach is taking Time-to-Live and transmission delay time considerations as key parameters. Here the hop count value is the modification of final TTL value and initial TTL value which is paralleled with stored Hop Count.

References

[1] Narendra Mishra and R. K. Sing.h "Detection of DDoS Vulnerability in Cloud Computing Using the Perplexed Bayes Classifier" Hindawi Computational Intelligence and Neuroscience Volume 2022 , Article ID 9151847, 13 pages https://doi.org/10.1155/2022/9151847.

[2] Ammarah Cheema and Moeenuddin Tariq et. al., "Prevention Techniques against Distributed Denial of Service Attacks in Heterogeneous Networks: A Systematic Review" Hindawi Security and Communication Networks Volume 2022, Article ID 8379532, 15 pages https://doi.org/10.1155/2022/8379532.

[3] Mishti D. Samani and Miren Karamta et. al., "Intrusion Detection System for DoS Attack in Cloud" *International Journal of Applied Information Systems* (IJAIS) – ISSN : 2249-0868, Foundation of Computer Science FCS, New York, USA Volume 10 – No. 5 (2022). February 2016 – www.ijais.org

[4] Afra Domeke and Bruno Cimoli et. al., "Integration of Network Slicing and Machine Learning into Edge Networks for Low-Latency Services in 5G and beyond Systems"Appl. Sci., 12, 6617 (2022). https://doi.org/10.3390/app12136617.

[5] Meghna Chakraborty and Timothy Gates. "Causal Analysis and Classification of Traffic Crash Injury Severity Using Machine

Learning Algorithms" 8th Road Safety & Simulation International conference RSS (2022).

[6] Gayatri K. Chaturvedi and Arjun K. Chaturvedi, et.al "A study of Intrusion Detection System for Cloud Network Using FC-ANN Algorithm" *International Journal of Engineering Development and Research* 2016 IJEDR | Volume 4, Issue 3 | ISSN: 2321-9939

[7] Chida Nanda Murthy P., Dr. A. S. Manjunatha, AnkuJaiswal, Madhu B. R.; "Building Efficient Classifiers For Intrusion Detection With Reduction of Features"; ISSN 0973-4562 Volume 11, Number 6, pp 4590-4596 (2016).

[8] Snehal G. Kene "A Review on Intrusion Detection Techniques for Cloud Computing and Security Challenges" IEEE Sponsored 2nd International Conference On Electronics And Communication Systems (ICECS '2015) 978-1-4244-xxxx-x/09 ©2009 IEEE.

[9] Rabi Prasad Padhy and Manas Ranjan Patraet. Al "Cloud Computing: Security Issues and Research Challenges" *International Journal of Computer Science and Information Technology & Security* (IJCSITS) Vol. 1, No. 2 (December 2011) ISSN: 2249-9555.

[10] Janu, Neha, et al. "Multiple Watermarking Scheme for Video & Image for Authentication & Copyright Protection." IOP Conference Series: Materials Science and Engineering. Vol. 1131. No. 1 (2021). IOP Publishing.

[11] Kumar, Ashutosh, et al. "Virtual environments testing in cloud service environment: a framework to optimize the performance of virtual applications." *International Journal of System Assurance Engineering and Management* 13.1 : 1-15 (2022).

[12] Yadav, Sunil, et al. "Improvisation Of Data Mining Techniques In Cancer Site Among Various Patients Using Market Basket Analysis Algorithm." BEST: *International Journal of Management, Information Technology and Engineering* (ISSN: 2348-0513) Volume 3 (2015).

[13] Sharma, Gajanand, et al. "Self-healing topology for DDoS attack identification & discovery protocol in software-defined networks." *Journal of Discrete Mathematical Sciences and Cryptography* 24.8 : 2221-2232 (2021).

[14] Sharma, Gajanand, et al. "Video tempering detection assessment in full reference mode using difference matrices." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 645-659 (2019).