International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol. 9, Issue.3, March 2021 E-ISSN: 2347-2693

Correlation Based Mechanism for the Detection of DDOS Attack

Simmi[1*], Harjinder Kaur[2]

[1,2]Computer Engg, Swami SarvaNand College of Engg and Technology, PTU, Dina Nagar, India

**Corresponding Author: simmigsp89@gmail Tel.: 6239747574*

DOI: https://doi.org/10.26438/ijcse/v9i3.1822 | Available online at: www.ijcseonline.org

Received: 10/Mar/2021, Accepted: 17/Mar/2021, Published: 31/Mar/2021

Abstract— As technology is blooming cloud computing becomes indispensible part of many companies. The users are dependent upon cloud infrastructure as it is widely adopted and used technology. In cloud computing the prime concern is shared storage and it has many security issues. One of these security issues is DDOS attack that can effect business organization which utilizes cloud. This paper describes an approach to handle DDOS attack in cloud systems. In the proposed approach Interpolation between the values are located. In the proposed approach, security attributes gives highest Interpolation and reliability is the next highest Interpolation values. Both of these attributes serve as root nodes. The comparison between these attributes and training data is made to determine the DDOS attack. This means complication of calculations is reduced. Execution time is greatly reduced using this procedure. Results obtained are similar but execution time is reduced. The mechanism of ordering and normalization gives the hierarchical clustering.

Keywords— cloud computing, DDOS attack, Interpolation

I. INTRODUCTION

The DDOS attack in computer security is an attack wherein a reputation system is subverted by forging identities in cloud environment. It is named after the subject of the book DDOS, a case study of a woman diagnosed with dissociative identity disorder.

A DDOS attack is a Multiple Identity Attack utilizing multiple distributed attack sources. Typically, the attackers use a large number of controlled bots distributed in different locations to launch a large number of Multiple Identity Attack attacks against a single target or multiple targets. With the rapid development of cloud technology in recent years, the attack traffic scale caused by Multiple Identity attacks has been increasing, with the targets including not only business servers, but also internet infrastructures such as firewalls, routers and DNS system as well as cloud bandwidth, the attack influence sphere has also become broader.[1]Cloud computing by all accounts is an evolution which is gaining a push by inheriting features of grid and utility computing, hardware virtualization, Web 2.0 Service Oriented Architecture (SOA) and autonomic computing.

The practicability of this computing model is to create unrivaled and proficient utilization of distributed resources and then clubbing them together with a specific goal to confront user defined requests and provide them best quality services [2]. Cloud computing is one of the type of computing system which consists of different virtualized and inter-connected resources which are provisioned on-demand and appeared to be as one integrated computing resource based on Service Level Agreement [3]. Cloud computing offers a provision to access a shared pool of computing resources which incorporates storage room, calculation control, hardware, applications and administrations on request premise to the clients over the web. The user no longer need to worry about the initial investments on the resources with same ease as utilizing common utilities such as natural gas, water, electricity supply on pay per use bases by ensuring Quality of Services at the same time. [4]Cloud provides a wide range of computing resources from servers and storage to enterprise applications. Cloud is a hosting environment that is immediate, flexible, scalable, secure and available. The computing resources from cloud can be easily and quickly accessed and released after use with very less management effort. This paper introduces an effective method to detect and remove a DDoS attack in cloud. DDOS attack will be the one in which one node takes the identity of other node. The overall performance goes down by the application of DDOS attack. In order to resolve the problem Euclidean distance mechanism is merged along with Interpolation and NN approach. NN used to find the neighbours of the node being analysed. This handles DDOS attack effectively and reduces the execution time. The rest of the paper is organized as under: section 2 gives the literature survey involving DDOS handling approach, section 3 gives the methodology of work, section 4 gives the performance analysis and result, section 5 gives conclusion.

II. LITERATURE SURVEY

[5]proposed a generalized attack detection model that utilizes the spatial Interpolation of received signal strength inherited from wireless nodes. The suggested work provide a theoretical analysis of our approach. It derived the test statistics for detection of identity-based attacks by using the K-means algorithm. The proposed attack detector is robust when handling the situations of attackers that use

different transmission power levels to attack the detection scheme. We further describe how we integrated our attack detector into a real-time indoor localization system, which can also localize the positions of the attackers. Identity based attack detection process uses detection but blocking process is missing. Median error can still be minimized.

[6]In this paper protocol specific DDOS attack detection mechanism is proposed. The mechanism detects the DDOS attack based on protocol observing the flow of distribution of traffic. Cloud environment is considered for evaluating the behaviour of the attack. The attack is primarily on data-centers and transmitted packets. Packets are labelled and stored within the Queue. The queue is arranged according to the preference and queue having highest priority packets are transmitted at first place. Execution time is not observed that is a issue that is to be rectified in the proposed work.

[7] In this paper, a distributed method has been presented using mobile agents and local information of each sensor to detect DDOS attack. The method presented in this paper re- moves the adversary nodes from participation in routing while using mobile nodes and increases the security in cloud. This work improves packet drop ratio but intrusion detection and blocking of nodes being is missing hence further improvement in terms of blocking by establishing threshold in not done. Hence throughput can further be improved.

[8]proposed a fully distributed and effective scheme that randomly drops extra PKC request messages beyond its processing capability. This approach is not only resistant to PKC-based DoS attacks, but also energy-efficient. The residual energy is not considered hence by considering this energy effect further energy consumption can be minimized.

[9]proposed a source-authenticated broadcast encryption scheme by fixing the identity-based broad- cast encryption scheme. The security of this scheme is proved in the random oracle model. Analysis of our scheme shows that it is comparatively efficient in terms of computation and communication. Key based approach is used in which energy consumption art source end is high. Energy consumption in resource constraint environment can further be minimized.

[10] The proposed scheme, does not need issuing a third-party query to certificate authority (CA). Moreover, it eliminates the key escrow problem, an important constraint in Identity-based digital signatures. Also, the sender has the ability to update its keys without changing its identity whenever necessary. Digital signatures scheme is one of the most secure schemes to ensure attack prevention. This approach is sender based however intermediate attacks can occur and also energy consumption is high.

[11] The so-called indirect DDOS attack is the main focus of this study. A performance analysis is devised, where the expected potential number of indirect DDOS nodes in randomly deployed Clouds is computed. Moreover, the probability of an (indirect) DDOS-free sensor cloud is calculated subject to the number of sensor nodes and the sensor area intensity. Specific sensor nodes are dealt with in this approach. The mobility issue as an extended feature of this model in an attempt to enable a more sophisticated DDOS attack detection tool for a wide variety of sensor cloud applications can be done.

[12] proposed the optimization technique i.e. Bacterial Foraging optimization is applied individually on DSR routing protocol and then compare the performance analysis of DSR routing protocol through BFO approach and without BFO approach that performs better to increase the lifetime of the Cloud services so that packets will be transferred in an efficient manner and with less error rate so that the chance of node failure will be less and prolong the lifetime of the services for the realization of routing optimization. Network lifetime is extended by reducing the packet drop rate.

The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility.

III. PROPOSED WORK

In this we consider the problem of approximating a given function by a class of simpler functions, mainly polynomials. There are two main uses of interpolation or interpolating polynomials. The first use is reconstructing the function X_i when it is not given explicitly and only the values of X_i and/or its certain order derivatives at a set of points, called nodes, tabular points or arguments are known. The second use is to replace the function X_i by an interpolating polynomial Y_p so that many common operations such as determination of roots, differentiation and integration etc. which are intended for the function X_i may be performed using Y_p. A polynomial Y_p is called an interpolating polynomial if the value of Y_p and/or its certain order derivatives coincides with those of X_i and/or its same order derivatives at one or more tabular points. It extracted the features and then added it into polynomial Y_p. This calculated value is compared against each other and attack is predicted.

Algorithm Interpolation Based DDOS

a. Read number of data (n) from dataset
b. Read data X_i and $Y_i$from dataset for i=1 to n
c. Read value of independent variables sayxp whose corresponding value of dependent say yp is to be determined.
d. Initialize: yp = 0
e. For i = 1 to n

Set p = 1
For j =1 to n
If $i \neq j$ then
Calculate $p = p * (xp - X_j)/(X_i - X_j)$
End If
Next j
Calculate $yp = yp + p * Y_i$
Next i

f. Display extracted feature and add this feature toyp as interpolated value.

g. Compare the calculated values and predict the DDOS attack.

The demonstration of this approach is described in this section. First of all we consider example 1 and then provide explanation of the same.

Example 1: Traffic is analyzed using protocols applied on dataset. This dataset used for traffic distribution is as under

Table 1: Demo Dataset

Traffic(X)	Time(Y)
0	1
1.386294	4
1.791760	6

Time 1:00 AM or PM is represented in normalized form as 1.
During training it is suggested that traffic under 0.5 is not intruder. In case traffic exceeded 0.5 then intrusion is detected.

The approach first of all builds a difference table and then apply the Interpolation approach to calculate the value that is abnormal. The overall procedure is as under
The first-order polynomial can be used to obtain the estimate at Time(Y) = 2,

f_1 1.386294 = 0.4620981

Since value is less then 0.5 hence intrusion is not detected at 2 PM
In a similar fashion, the second-order polynomial is developed as

$$f_2(2) = \frac{(2-4)(2-6)}{(1-4)(1-6)}\ 0\ 1.386294 + \frac{(2-1)(2-4)}{(6-1)(6-4)}\ 1.791760 = 0.56$$

Value is greater than 0.5 and hence intrusion is detected.

Proposed Approach(Interpolation based DDOS Attack detection)

In the proposed approach Interpolation between the values are located. Each attribute is distinctly evaluated. The highest Interpolation values are maintained at the root and attributes having least values serve as child nodes. Interpolation calculated twice. In the proposed approach, security attributes gives highest Interpolation and reliability is the next highest Interpolation values. Both of these attributes serve as root nodes. The comparison between these attributes and training data is made to determine the DDOS attack. This means complication of calculations is reduced. Execution time is greatly reduced using this procedure.

1.386294 = 0.4620981

Here no need to take first identity since it is low traffic zone and chances of intrusion are negligible. Results obtained are similar but execution time is reduced. The mechanism of ordering and normalization gives the hierarchical clustering.

IV. RESULT AND DISCUSSION

DDOS attack will be the one in which one node takes the identity of other node. The overall performance goes down by the application of DDOS attack. In order to resolve the problem Euclidean distance mechanism is merged along with Interpolation. Euclidean distance used to find the neighbors of the node being analyzed. In case there exists only one neighbor of current node then DDOS attack is detected. The Euclidean distance is used to check the location of the DDOS node. The overall time consumption of simulation is achieved to be better as compare to existing approach. This is shown as under

A. Result in terms of classification accuracy

The classification accuracy indicates the difference between the actual value and approximate value. The mechanism employed calculates the values of Interpolation between each and every attributes. The result is mentioned within the table 3

Table 2:Classification Accuracy Comparison

Number of Rows	Classification Accuracy(Base)%	Classification Accuracy(Proposed) %
1000	90	98
2000	92	98
3000	93	99
4000	94	99
5000	95	99
6000	90	99+

The classification accuracy comparison indicates that the proposed mechanism has significant high accuracy as compared to existing mechanism. This is also indicated through the following plots

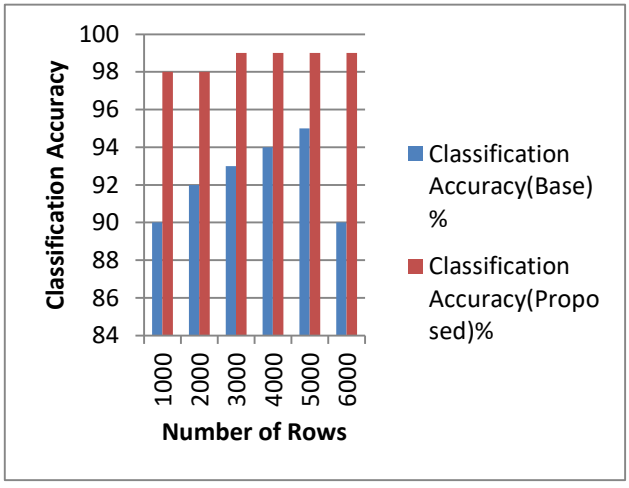

Figure 1: Classification Accuracy comparison

B. Interpolation Comparison

There are number of distinct attributes present within the dataset. The Interpolation between different attributes is evaluated and highest Interpolation values are retained. The result obtained are given in this section as

Interpolation between Attribute 1 and DDOS(DDOS)

Table 3: Comparison between the DDOS and first attribute of dataset

• Attribute	• Interpolation
• Attribute 1 and DDOS	• 0.34

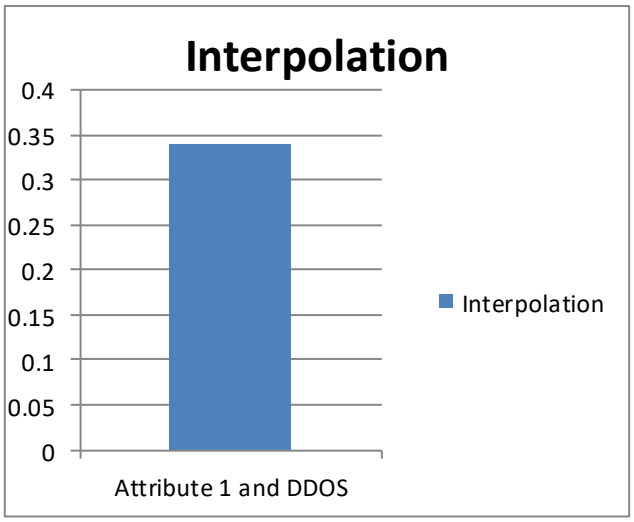

Figure 2: Interpolation between the DDOS and attribute 1

This Interpolation value indicates that the Interpolation is 0.34 for the proposed mechanism.

The next Interpolation is obtained with the second attribute and DDOS. This is given in the table 5.

Interpolation between Attribute 2 and DDOS

Table 4: Comparison between the DDOS and second attribute of dataset

• Attribute	• Interpolation
• Attribute 2 and DDOS	• 0.38

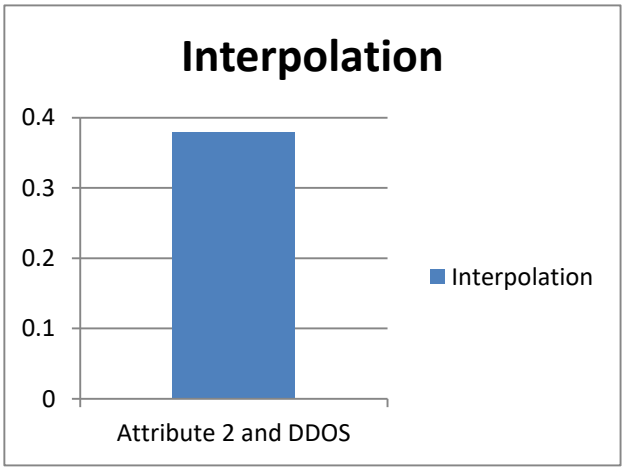

Figure 3: Interpolation between the DDOS and attribute 3

This Interpolation value indicates that the Interpolation is 0.38 for the proposed mechanism. In addition classification accuracy of the proposed system is more than 99%. This proves the worth of the study.

V. CONCLUSION AND FUTURE SCOPE

The proposed work efficiently analyses the DDOS attack. Strategy to tackle DDOS attack is suggested. The mechanism that is used in the base paper is multithreaded queue based approach. In that approach the main problem is the classification accuracy problem. This is caused since all the attributes must be matched with the training data. Interpolation calculated twice. In the proposed approach, security attributes gives highest Interpolation and reliability is the next highest Interpolation values. Both of these attributes serve as root nodes. The comparison between these attributes and training data is made to determine the DDOS attack. This means complication of calculations is reduced. Execution time is greatly reduced using this procedure.

REFERENCE

[1] K. Kim, M. Erza, A. Harry, and C. Tanuwidjaja, *Network Intrusion Detection using Deep Learning A Feature Learning Approach*. **2018.**

[2] W. Kong, Y. Lei, and J. Ma, "Data security and privacy information challenges in cloud computing," *Int. J. Comput. Sci. Eng.*, **vol. 16, no. 3, pp. 215–218, 2018.**

[3] S. A. Repalle, V. R. Kolluru, and 2, "Intrusion Detection System using AI and Machine Learning Algorithm," *Int. Res. J. Eng. Technol.*, **vol. 4, no. 12, pp. 1709–1715, 2017.**

[4] Z. Zhou, C. Du, L. Shu, G. Hancke, J. Niu, and H. Ning, "An Energy-Balanced Heuristic for Mobile Sink Scheduling in Hybrid WSNs," *IEEE Trans. Ind. Informatics*, **vol. 12, no. 1, pp. 28–40, 2016.**

[5] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, **vol. 59, no. 5, pp. 2418–2434, 2010.**

[6] S. G. Hersha, Rajendra Patil, "Protocol Specfic Multi Threaded Network Intrusion Detection System(PM-NIDS) for DOS/DDOS attack detection in cloud," *IEEE ACcess*, **2018.**

[7] S. Moradi, "A distributed method based on mobile agent to detect Sybil attacks in wireless sensor networks," *IEEE Access*, **pp. 276–280, 2016.**

[8] D. Kim and S. An, "PKC-based dos attacks-resistant scheme in wireless sensor networks," *IEEE Sens. J.*, **vol. 16, no. 8, pp. 2217–2218, 2016.**

[9] M. Luo, C. Zou, and J. Xu, "An efficient identity-based broadcast signcryption scheme," *J. Softw.*, **vol. 7, no. 2, pp. 366–373, 2012.**

[10] S. Sadrhaghighi and I. T. Engineering, "Detect Pollution Attacks in Intra-Session Network Coding," **pp. 7–12, 2016.**

[11] P. Sarigiannidis, "Analysing Indirect Sybil Attacks in Randomly Deployed Wireless Sensor Networks," *IEEE Access*, **pp. 0–5, 2016.**

[12] S. Mahajan, "A Mechanism of preventing Sybil Attack in MANET using Bacterial Foraging Optimization," *IEEE Access*, **pp. 4–8, 2016.**

AUTHORS PROFILE

Miss simmi pursed Bachelor of Science from Beant college of Engineering and technology,Gurdaspur in 2018 and currently pursuing Master of Science from Swami Sarvanand Group of Institutes, DinaNagar Punjab since 2018. This is my first paper that iam publishing in international journals computer science and Engg.

Mrs Harjinder Kaur pursed Bachelor of Science from PTU campus, kapurthala and Master of Science in cse from BCET, Gurdaspur. She is currently working as Assistant Professor in Department of CSE, Swami Sarvanand Group of Institutes,DinaNagar Punjab.She has 12 years of teaching Experience in the Field of Computer Science and Department.

