International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Multiple Identity Attack Detection using Correlated Ensemble based Approach

Pooja Prasher

Abstract

An DDOS 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. 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 DDOS detection using special mining procedure of neural network is proposed through this literature. This paper describes an approach to handle DDOS in cloud systems. .In the proposed approach correlation between the values are located and the security attributes gives highest correlation and reliability is the next highest correlation values. Both of these attributes serve as root nodes. The comparison between these attributes and training data is made to determine the DDOS. This means complication of calculations is reduced. Classification accuracy of the proposed work is increased considerably..

Keywords: DDOS, DNS System, Correlation

i. Introduction

The DDOS 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 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.[1] 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.[2]

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 [3]. 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 [4]. 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. [5]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 in cloud. DDOS will be the one in which one node takes the identity of other node. The overall performance goes down by the application of DDOS. In order to resolve the problem Euclidean distance mechanism is merged along with correlation and NN approach. NN used to find the neighbours of the node being analysed. This handles DDOS 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

Cloud is vastly used area and distinct users interacting with it. In order to resolve the problem associated with attacks in Cloud various techniques are proposed. This literature studies such mechanisms.

Y.Chen et al.[6](2010) Proposed a generalized attack detection model that utilizes the spatial correlation 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.

S.G.Hersha et al.[7] (2012) presented a protocol specific DDOS detection mechanism is proposed. The mechanism detects the DDOS 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-centres 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.

[8] In this paper, a distributed method has been presented using mobile agents and local information of each sensor to detect DDOS. 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 DDOS 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.

[9]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.

[10]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.

[11] 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.

iii. Proposed System

The proposed system uses the hierarchical clustering mechanism to improve the classification accuracy and

reduce false positive rate. The false negative rate is minimized by the use of hierarchical clustering procedure. The procedure detects the DDOS with precision and accuracy. The hierarchical clustering procedure builds clusters based on closest pairs. Each clusters is formed by selecting data that is not related with each other. After this closest clusters are merged together. This process continues until no more data is left for distinguishment.

Algorithm Used

The methodology to achieve the objectives is listed as follows

1. Input the number of nodes in the clouds.
2. Enter the threshold Correlation(Ct) associated with node.
3. Initialize count=0
4. Check the neighbourhood of nodes in terms of coverage area(Ci)
   4.1 if Ct>Ci then
   Count=count+1
   Store packets in Queue
   End of if

EXISTING RESEARCH

5. if count=1 then
   5.1 Apply Euclidean distance to determine location of attacking node
   5.2 If Ct>Ci then
   5.3 Declare DDOS along with its location
   End of if

Changes to existing research

6. Repeat the above steps for all the nodes
7. Calculate Classification accuracy
8. Stop

Description

Traffic is analysed using protocols applied on dataset. This dataset used for traffic distribution is as under

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

Table 1: Demo Dataset

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 DDOS is detected.

The approach first of all builds a difference table and then apply the correlation 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,

$$f_1(2) = \frac{2-4}{1-4}\,0 + \frac{2-1}{4-1}\,1.386294 = 0.4620981$$

Since value is less then 0.5 hence DDOS is not detected at 2 PM

In a similar fashion, the second-order polynomial is developed as

$$f_2(2) = \frac{(2-4)(2-6)}{(1-4)(1-6)}\,0 + \frac{(2-1)(2-6)}{(4-1)(4-6)}\,1.386294 + \frac{(2-1)(2-4)}{(6-1)(6-4)}\,1.791760 = 0.5658444$$

Value is greater than 0.5 and hence DDOS is detected.

Proposed Approach(Hierarchical Clustering)

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

$$f_1(2) = \frac{2-1}{4-1}\,1.386294 = 0.4620981$$

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

iv. Result and Discussion

DDOS will be the one in which one node takes the identity of other node. The overall performance goes down by the application of DDOS. In order to resolve the problem Euclidean distance mechanism is merged along with correlation and NN approach. NN used to find the neighbours of the node being analysed. In case there exists only one neighbour of current node then DDOS 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

7.1 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 correlation between each and every attributes. The result is mentioned within the table 3

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+

Table 2:Classification Accuracy Comparison

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

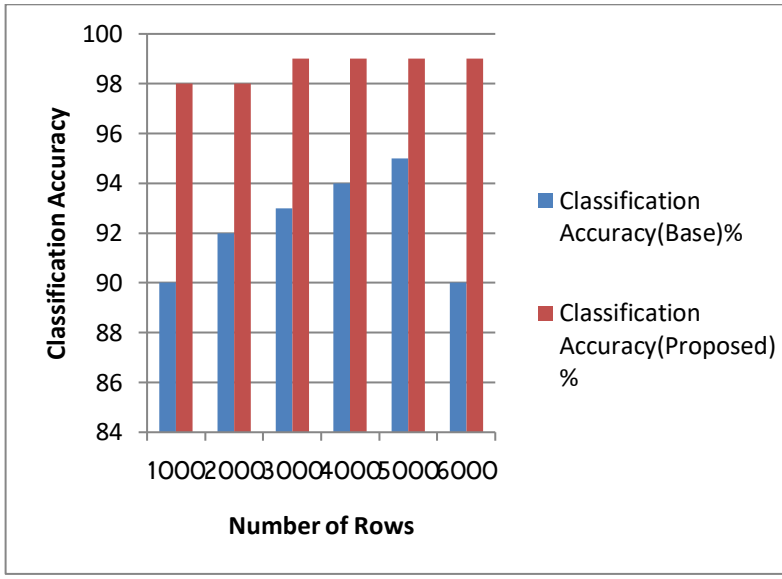

Figure 1: Classification Accuracy comparison

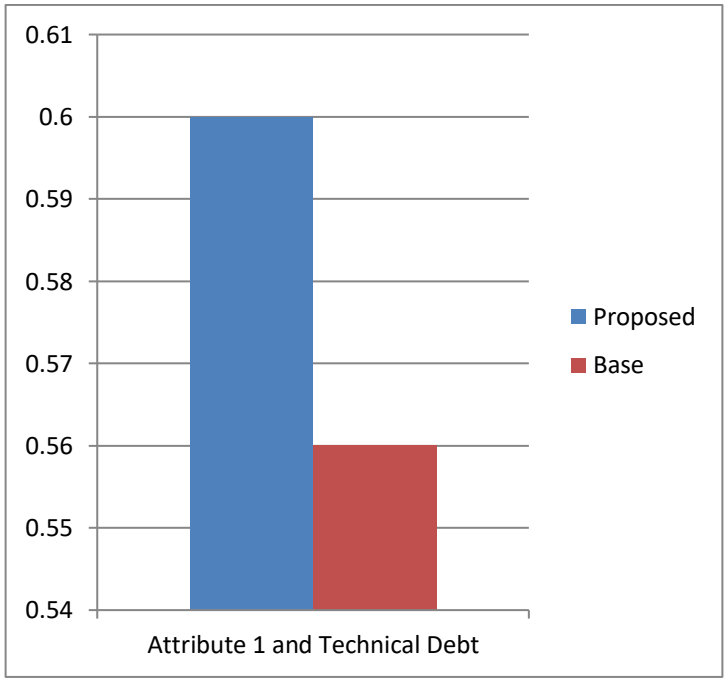

Figure 2:Correlation between the technical debt and attribute 9

This correlation value indicates that the correlation is 0.60 for the proposed mechanism. From the result section it is clear that security and reliability attribute has highest correlation values and from the correlation values nodes are recruited as root nodes. The test data is than compared against the train data to form the finalize result in terms of DDOS.

V. Conclusion

The proposed work efficiently analyse the DDOS. Strategy to tackle DDOS 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. If match occurs than result is predicted. But in case even a single mismatch occurs than classification error occurs. To rectify the issue,in the proposed approach correlation between the values are located. Each attribute is distinctly evaluated. The highest correlation values are maintained at the root and attributes having least values serve as child nodes. Correlation calculated twice. In the proposed approach, security attributes gives highest correlation and reliability is the next highest correlation values. Both of these attributes serve as root nodes. The comparison between these attributes and training data is made to determine the DDOS. This means complication of calculations is reduced. Execution time is greatly reduced using this procedure.

References

[1] K. M. Akhil, M. P. Kumar, and B. R. Pushpa, "Enhanced cloud data security using AES algorithm," *Proc. 2017 Int. Conf. Intell. Comput. Control. I2C2 2017*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/I2C2.2017.8321820.

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

[3] 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, doi: 10.1504/IJCSE.2018.091772.

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

[5] 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, doi: 10.1109/TII.2015.2489160.

[6] 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, doi: 10.1109/TVT.2010.2044904.

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

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

[9] 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, doi: 10.1109/JSEN.2016.2519539.

[10] M. Luo, C. Zou, and J. Xu, "An efficient identity-based broadcast signcryption scheme," *J. Softw.*, vol. 7, no. 2, pp. 366–373, 2012, doi: 10.4304/jsw.7.2.366-373.

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