International Journal of Computer Trends and Technology
ISSN: 2231 – 2803 / https://doi.org/10.14445/22312803/IJCTT-V69I5P108

Volume 69 Issue 5, 55-59, May 2021

Original Article

DDoS Malicious Node Detection by Jaccard and Page Rank Algorithm in Cloud Environment

Adil Hussain Mohammed

DC Access System (DCAS) Linux Engineer &Department of Health Care Finance (DHCF)
DHCF's headquarters 955 L'Enfant Plaza, SW, 3rd Floor, Washington, DC 20024.

Received Date: 14 April 2021
Revised Date: 27 May 2021
Accepted Date: 31 May 2021

Abstract *- Cloud infrastructure increases the strength of service and product based companies by serving more users with limited infrastructure. Many of researcher are working to improve the security of vulnerable cloud infrastructure. This paper has proposed a trust based model for detection of DDoS attacked malicious nodes in the network. Based on node resource uses in the network a belief was developed by the cloud bridge. Further paper evaluates jaccard coefficient trust value based on transaction happens between nodes. This jaccard coefficient is social feature calculate as per node behavior with all other nodes. Finally a cumulative trust was estimate by page rank method using jaccard and initial belief model. Experiment was done on DDoS attack network. Result shows that proposed model has increases the malicious node detection.*

Keywords *- Cloud computing, Jaccard Coefficient, Page Rank, Classification, Trust Model.*

I. INTRODUCTION

Companies are eventually changing their IT strategies and are turning towards the cloud to meet their data storage requirements to improve their scalability and to reach globally. There are several benefits of cloud computing among which the major ones are lower cost, fault tolerance, flexibility, and efficient response to the latest business needs. But with the advent of this new technology brings new threats and challenges as concerned with the privacy of data that is processed or stored within the cloud. Out of which one of the major challenges of cloud computing is that the consumers who are the actual owners of information while sending their information into the cloud lose control of their precious data. This increases the chances of information theft considerably. Cloud computing indeed offers many benefits but steps have to be taken to improve the trust of people in cloud computing to ensure that the information stored in it is private and confidential.

One of the problems with cloud computing is the management and the owners of the website hosting services are removed from the control of a solitary owner. And many important organizations such as government agencies, financial institutes, and health care providers are lawfully required to keep their data secure. Normally such organizations maintain their own data centers to keep their data safe and secure. Such organizations cannot move towards the cloud due to the risk of a data leak that they cannot control.

Particularly, data storage is important service. Despite the fact that many enterprises and organizations would want to keep their information in their own framework because of security and trust reasons, the use of cloud on data storage and sharing is genuinely prominent [5]. Included system providers give diverse types of security of records and the system, however they are not generally thought to be adequate as there are a wide range of requirements relying upon the clients. It is, in any case, in near future expected to be common [6]. This model gives different sorts of security services in various forms. The trust in cloud computing is partitioned into different classes specifically Reputation Based Trust, SLA check based trust, Policy-based trust, Evidence-based trust and Societal trust [4, 5].

II. RELATED WORK

Rafey et al. [7] calculated the trusted nodes based on the behavior of the node. In his representation transaction attributes of nodes such as confidence, power, context importance, and social attributes such as relationship, centrality, and friendship were considered to calculate the overall trust value of the machines. The trust based accuracy given by this model is affected by results from dishonest nodes.

Chen et al. [8] In this model consider both the QoS also the trust metrics that include energy status and also the reputation in terms of quality together with social trust metrics. But for some reason, this study was not considered to achieve perfect results.

Pei Yun Zhang et al. [9] proposed a trust model related to the algorithm to decrease the trust management load and worked to improve the node detection ability that was

malicious on the domain partition. Partitioning such nodes into domains was helpful to decrease the load of trust managing in terms of computation and storage. Cross-domain sliding of windows and domain were proposed and were used to save the latest trust values. After this, an algorithm was designed to compute the cross-domain and domain trust value of the nodes, a procedure called filter was applied to remove the malicious nodes and malicious trust evaluations from the domain.

D. Eyers et. al. in [10] A camFlow model as a trial was launched in data-centric model in the PAAS cloud was also proposed by the authors. It enforces the data flow strategy and executes the information between the machines at the hardware kernel part while exchanging of the messages.
Z. Wu et. al. in [11] Two-layer data flow model was again adopted for the cloud that provides data flow tracking and controlling which was proposed as a protection mechanism from system attacks like buffer and stack overflow.

N. E. Moussaid et. al. in [12] Security attributes were formulated in a dynamic fashion when the behaviors of these collected entities were linked with security classes and trust level and it also enhanced the information flow together with security control. It was difficult to identify the information flow boundary due to the sharing of machines (virtual).

X. Lu et. al. in [13] also proposed a control method that was dynamic and was used to know the virtual boundary recognition by sensitive information flow. It combines the concepts of decentralized and centralized information flow control.

Omar Abdel Wahab et. al. in [14] Two-fold type solution was also adopted that allows the hypervisor to make a trust relationship with the guest virtual machines by knowing the subjective and objective trust resources and employing them with Bayesian inference to combine them. We design a game that was trust based among the hypervisor that tries to maximize the minimization that was caused to a cloud system by DDoS attackers under the inadequate budget of the resources. This game control the hypervisor to detect the load distribution in real-time among VMs that maximizes attacks and detects the DDoS.

III. PROPOSED METHODOLOGY

Proposed model Jaccard Coefficient and Page Rank Trust Model (JCPRTM) was detained in this section of paper. Each node have processor, memory (RAM) and bandwidth resource. Cloud bridge maintain resource utilization data with number of successful and unsuccessful transaction. This model calculates trust value by utilizing jaccardcoefficient and page rank methods. Proposed model steps were shown in fig. fig. 1. Various elements of the model were explains below.

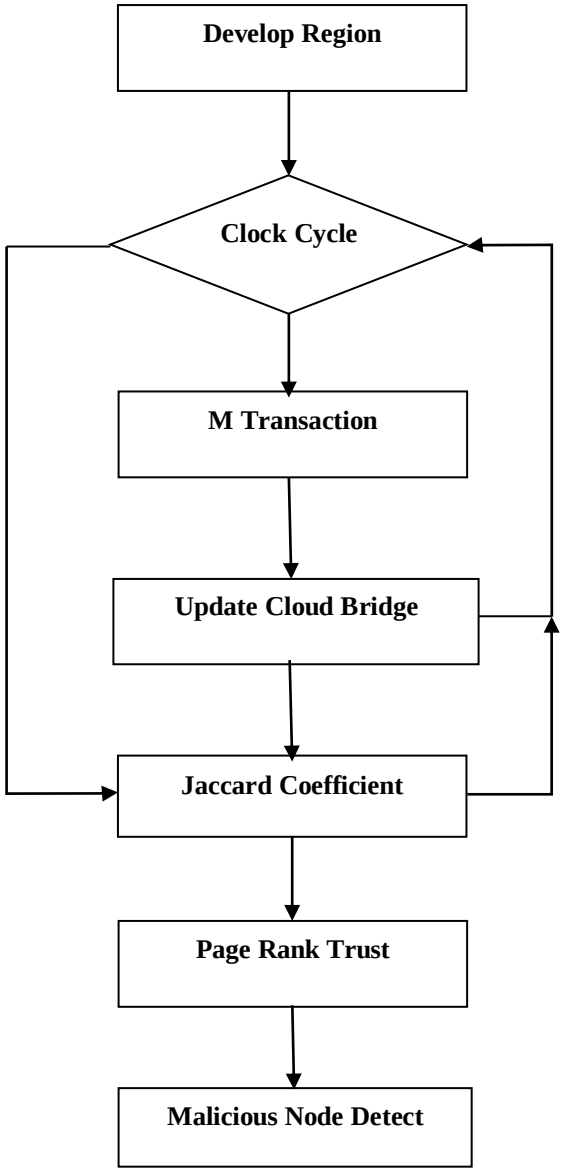

Fig. 1 Proposed work training module

A. Clock Cycle

Cloud defines a fix size time range as a clock. So in one clock cycle more than one node may initiate a transaction. Clock cycle (CC) is definite number of clock count for updating a trust value of nodes at cloud bridge table.

B. Initial Belief

As per node resource utilization initial belief value was estimate. If node have no over resource utilization the its initial belief value if 1. If node have one or more over resource utilization then sum of all over utilization resources ratio ($R_{limit}/R_{over\_Use\_Percent}$) [14].

$$I_j = \begin{cases} 1 \; if \; \mathrm{R_{i,Limit}} > \mathrm{R_{i,Over\_Use\_Percent}} \text{ for i} = \{1 \ldots \mathrm{r}\} \\ \sum_{i=1}^{r} \mathrm{R_{i,Limit}} / \mathrm{R_{i,Over\_Use\_Percent}} \; otherwise \end{cases}$$

Where $R_{r,limit}$ is limit for r^{th} resource of node j, similarly $R_{r,over\_Use\_Percent}$.

C. Node Trust value

Each node in the cloud has a trust value range from 0 to 1. This value may increase or decrease as per the behavior of the nodes in form of transaction success. Cloud bridge storage tables were used to evaluate this value of work. First was evaluation of node direct trust value where number of successful transaction counts were divide by total number of transaction.

So let successful transaction count between i, j node is represent by Ts_{ij} and total number of transaction represent by Tt_{ij}[15]. Estimation of direct trust value was done Eq..

$$D_{ij} = \frac{Ts_{ij}}{Tt_{ij}}$$

Above eq. 1 gives n number of direct trust value for each node, but behaviors of node with node may be different. As malicious node provide good service to some node and poor service to others. So this trust value needs to be further process by jaccard coefficient function. This function takes all direct trust value of a node and generates a single value of the node as per different beahvious operations done by node with other nodes.

D. Jaccard Coefficient

Jaccard function was proposed by [16] where as per various observed features between two element a trust value was generate by Eq.

$$JC = \frac{A \cap B}{A \cup B}$$

In above eq. A, B are nodes in the cloud and features are direct trust value between them. $A \cap B$ is obtained by getting lower direct trust value between A and B for same nodes like A→C, B→C. $A \cup B$ is obtained by getting higher direct trust value between A and B for same nodes like A→C, B→C.

E. Page Rank Trust

Jaccard values are utilize to get the page rank [17] value of each node. Rank of one node modify the other, hence behavior of node with other node effect the cumulative trust value.

$$PRT_i = \frac{\sum_{j \epsilon s} JC_j + I_j}{|s|}$$

Where s is subset of nodes having transaction with i node. I_j is initial belief of node.

F. Malicious Node Detection

Out of this page rank trust PRT help cloud to classify nodes into real and malicious node. Mean of PRT value was taken as threshold value. Nodes having higher PRT value as compared to threshold value was consider as real node while lower PRT value as compared to threshold value was consider as malicious node.

IV. EXPERIMENTS & RESULTS ANALYSIS

The experiment was done on a real dataset of research papers where different branch papers was taken to cluster the input dataset. Implementation of the proposed hybrid model was done on MATLAB software. Results were compared on the following evaluation parameters:

$$\mathrm{Pr}\,ecision = \frac{True\_Positive}{True\_Positive + False\_Positive}$$

$$\mathrm{Re}\,call = \frac{True\_Positive}{True\_Positive + False\_Negative}$$

$$F\_Score = \frac{2 * \mathrm{Pr}\,ecision * \mathrm{Re}\,call}{\mathrm{Pr}\,ecision + \mathrm{Re}\,call}$$

A. Results

Table 1. Precision value comparison of DDos attack node detection models.

Virtual Machine	DDos Malicious Nodes	JCPRTM	Previous Model [14]
25	5	0.3333	0.8125
30	5	0.3750	0.9167
30	8	0.3	0.6471
40	10	0.4286	0.7619

Table 1 shows that proposed JCPRTM model has increases the precision value as compared to previous model proposed in [14]. It was shown that use of jaccard coefficient increases the D-Dos malicious node detection accuracy of work. Combined use of different trust (jaccard and initial belief) in page rage rank has also improve the detection precision value.

Table 2. Recall value comparison of DDos attack node detection models

Virtual Machine	DDos Malicious Nodes	JCPRTM	Previous Model [14]
25	5	0.6667	0.8667
30	5	1	0.7333
30	8	0.75	0.8462
40	10	0.75	0.7619

Table 2 shows that proposed JCPRTM model has increases the recall value as compared to previous model proposed in [14]. It was shown that use of jaccard coefficient increases the D-Dos malicious node detection accuracy of work. Combined use of different trust (jaccard and initial belief) in page rage rank has also improve the detection recall value.

Table 3. F-Measure value comparison of DDos attack node detection models

Virtual Machine	DDos Malicious Nodes	JCPRTM	Previous Model [14]
25	5	0.444	0.8387
30	5	0.5455	0.8148
30	8	0.4286	0.7333
40	10	0.5455	0.7619

F-measure value shown in Table 3 is an inverse average precision and recall value. It was obtained that proposed model JCPRTM model has higher F-measure value as compared to previous model proposed in [14]. Cumulative use of jaccard coefficient and initial belief values in page rank method.

Table 4. Execution time value comparison of DDos attack node detection models

Virtual Machine	DDos Malicious Nodes	JCPRTM	Previous Model [14]
25	5	1.2218	0.3067
30	5	1.326	0.0324
30	8	1.3948	0.0328
40	10	2.8762	0.0239

Table 4 shows that execution time for malicious node detection of proposed model is less as compared to previous model [14].

V. CONCLUSION

Various network suffer from different type of attacks, some are easy to detect but may lead to heavy losses in terms of data, resource, etc. This paper has developed a DDoS attack detection model in cloud environment where nodes performing malicious activity are detect by trust evaluation technique. To get a node trust proposed model has monitor session between nodes either successful or un-successful. Jaccard coefficient model was used to get the collective trust values from other virtual machine. Further paper has utilizesjaccard value in page rank algorithm to get final trust value of the work. Experiemnt was done on different environment and results shows that proposed model ahs increased the malicious node detection accuracy. It was shown that use of jaccard coefficient increases the D-Dos malicious node detection accuracy of work. Combined use of different trust (jaccard and initial belief) in page rage rank has also improve the detection recall value. In future paper scholar can adopt other trust model by use of machine learning approach.

REFERENCES

[1] Manoj, K., Manglem, S. CBMIR: Content based medical image retrieval system using texture and intensity for eye images. International Journal of Scientific & Engineering Research, (2016).

[2] J. Heiser, and M. Nicolett, Accessing the Security Risks of Cloud Computing, G00157782, Gartner, Inc., Stamford, CT,(2008).

[3] M. Armbrust, A. Fox, It Griffith, et al., Above the Clouds: A Berkeley View of Cloud Computing, University of California Berkeley, Berkeley, CA, (2009).

[4] Zhang, Y. & Joshi, J. Access Control and Trust Management for Emerging Multidomain Environments. Annals of Emerging Research in Information Assurance, Security and Privacy Services, S. Upadhyay and R.O. Rao (eds.), Emerald Group Publishing, (2009) 421-452.

[5] Tingwei Chen, China Jing Lei. Research on Service Reputation Evaluation Method Based on Cloud Model. International Journal of Intelligent Information Systems 4(1) (2015) 8-15.

[6] I. Odun-Ayo, M. Ananya, F. Agono and R. Goddy-Worlu, Cloud Computing Architecture: A Critical Analysis, 2018 18th International Conference on Computational Science and Applications (ICCSA), Melbourne, VIC,(2018).

[7] Rafey S.E.A., Abdel-Hamid A., El-Nasr M.A. CBSTM-IoT: Context-based social trust model for the Internet of Things; Proceedings of the 2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT); Cairo, Egypt. 11–13 (2016)1–8.

[8] Chen Z., Ling R., Huang C.M., Zhu X. A scheme of access service recommendation for the Social Internet of Things. Int. J. Commun. Syst.(2016).

[9] Peiyun Zhang, Senior Member, IEEE, Yang Kong, And Mengchu Zhou. A Domain Partition-Based Trust Model For Unreliable Clouds. IEEE Transactions On Information Forensics And Security, 13(9)(2018).

[10] T. F. J.-M. Pasquier, J. Singh, D. Eyers, and J. Bacon, Cam_ow: Managed data-sharing for cloud services, IEEE Trans. Cloud Comput., 5(3)(2017)472-484.

[11] Z. Wu, X.-Y. Chen, and X.-H. Du, Enhancing sensitive data security based-on double-layer information _ow controlling in the cloud, Acta Electron. Sinica, 46(9)(2018) 2245-2250.

[12] N. E. Moussaid and M. E. Azhari, Enhance the security properties and information _ow control, Int. J. Electron. Bus., 15(3)(2020) 249-274.

[13] X. Lu, L. Cao, and X. Du, Dynamic control method for tenants sensitive information _ow based on virtual boundary recognition,IEEE Access, 8(2020)162548-162568.

[14] Omar Abdel Wahab, Jamal Bentahar, HadiOtrok, and Azzam Mourad. Optimal Load Distribution for the Detection of VM-based DDoS Attacks in the Cloud. IEEE Transaction, Services Computing (2020).

[15] Talal H Noor Quan Z Sheng Abdullah AlfaziJeriel Law and Anne HH Ngu Identifying fake feedback for effective trust management in cloud environments in Service Oriented Computing (2013) 47- 58.

[16] P. Jaccard. Etude comparative de la distribution orale dans une portion des alpes et des jura.Bulletin de la SocieteVaudoise des Science Naturelles, 37(1901).

[17] Larry, PageRank: Bringing Order to the Web. Archived from the original on May 6,(2002).

[18] Subburaj.V, & Srinivasan.M, & Surendiran, R & Sundaranarayanan, R. (2010). DDoS Defense Mechanism by Applying Stamps using Cryptography. International Journal of Computer Applications. 1(6), ISSN: 0975 – 8887, pp.48-52. DOI: 10.5120/143-262.