IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cloud Malicious Machine Detection Using Second Order Markov Model Trust

Nomaan Jaweed Mohammed

Abstract: Virtual machine incorporation increases the strength of cloud environment. Flexibility of user depends on easy availability of infrastructure at any instance during the service. This easiness brings many challenges that need to overcome and monitor continuously for the smoothness of cloud service. Out of different cloud issue this paper has resolved on malicious machine detection issue. Trust of virtual machines were evaluated by second order markov model, as per behavior noticed by the centralized datacenter. Trust value of each VM either old or new in cloud were evaluate after a fix time frame. This work dynamically adopt the sequential behavior among the machines as per assign job completion. Proposed model was robust against gray and distributed attacks. Experiment was done in these attacked environment and comparison of proposed model was done with existing techniques. Results shows that proposed second order markov model trust (SOMMT) has higher detection efficiency of malicious VM.

Index Terms— Data Mining, Cloud Computing, Markov Model, Trust Evaluation, Virtual Machine.

I. INTRODUCTION

Cloud computing is the future of the computing delivery model. It will be the next-generation network that will provide on-demand software and hardware services at a lower cost and lesser complexities [1]. There are too many users on the cloud and are performing their data transactions in the cloud environment and so the security of the data is crucial. The cloud should possess the quality to secure the data no matter how many applications are simultaneously running on the cloud. In the computer world, it is said that anything makeable can be breakable. It seems almost impossible that users trust cloud technology completely due to this reason. Therefore the main problem related to cloud computing is security and the providers will face that problem someday when the cloud will get bigger than the present. It will also be difficult for the users to find genuine cloud providers in the market where several cloud providers are present [2].

The management servers that are managed by the cloud providers are not completely trusted in unreliable clouds [3]. The cloud operators are those mediators who are hired by cloud providers to manage their clouds. Providers can be trusted in semi-trusted clouds but some of them may not be trusted as per the survey conducted in several reports [4]. The un-trusted cloud operators may use their privileges and can hack the management servers to attack the users' data and VM. They can execute commands to peek into the users' sensitive information and can also change them. They can also redirect the command of users to malicious VM. It is called a VM redirect attack and lies in the category of malicious-middle attack. The main reason behind this is the weakness of users' VMs and it is difficult to use the fact that only users can give the command to VM to redirect [5].

II. Literature Survey

Aluvalu and Muddana in [6] Built a control system related to trust obligation. The trust degree of the obligation can be improved with the help of obligation and the permission will de found out by role. Such popularity of combined service can help to tackle security and privacy issue.

Rohit and Bharat in [7] made a security system for the framework of web services to protect the integrity of data in the service life cycle. This solution will help users to get more control over their data with minimum risk of attacks.

Bhatia and Singh [8] Made a privacy model which contains parameters such as granularity level, retention period, privacy parameters, and environmental factors. Khaled and Zhu6 made a TB-AC trust control system based on 3 parameters as recommendations, attribute, and observations. Results showed that TB-AC can process the request within the specified time limit. Trust and risk are important factors and research is needed related to them in the cloud environment.

Nogoorani and Jalili [9] Made a framework in which the users' requests can be permitted or denied by several access policies. In this, the site administrator can give the user responsibility as an obligation.

Matin and Nima [10] gave the concept of control recognition and opinion leader which were output degree, reputation, and input degree based. This removes the troll entities factors from the cloud.

In [11] authors gave the paper related to decrease the trust overhead and improving the system for node detection for malicious or faulty nodes. It was good to partition the nodes in form of the domain to reduce the overhead of trust and will be helpful in computation and storage of trust. Cross-domain sliding windows and domain were given and were used to store the values of trust in nodes. Lastly to remove malicious nodes filtering was done.

In[12] an RTCM was made based on multisource feedback and also using fog computing fusion. At first, a new metric was introduced to the trust of the social sensor nodes while the sensing layer collects the trust value for detecting hazardous nodes. Second, fog computing devices collect the trust feedback values and useful trust calculation is done. This process hence reduces the delay in communication and overload of computing. Third, several different trust values were collected by a fusion algorithm which helps in improving the trust weights in both subjective and artificial weighting in ancient trust mechanisms.

In[13] mobile edge computing-based mechanism was used which evaluates the trust value in sensor nodes using the graphical model. It takes data from communication and collection behavior. Also, there is the scheduling of moving paths for the nodes to improve the direct trust and decrease the distance gap. This was an approximation algorithm and has proved its performance.

III. Proposed Model

In this section trust of virtual machine was evaluate by the steps follow in fig. 1. Working steps of block diagram was detailed separately. This paper has proposed a second order markov model trust (SOMMT). Some of notations used in the paper for explanation of proposed model was list in table 1.

Virtual Machine: Cloud is network of machines that provide services permanently or temporarily. So machine that provide services temporarily are term as virtual machine. In unreliable could machine have a trust value with as per performance in the network.

VM Sessions: Job assignment by a cloud to a VM_i from a VM_j is term as VM session. A VM Session has two state either success or Fail, in case of success VM_i complete assignment as per requirement. While in case of Fail, VM_j assignment was failed to complete. It was found that proposed model has utiized this parameter as core feature of a VM.

Centralized Datacenter: In order to record various activities of the virtual machine proposed model has stored data centrally in the Datacenter. This datacenter has utilized matrix data structure to arrange information like VM configuration

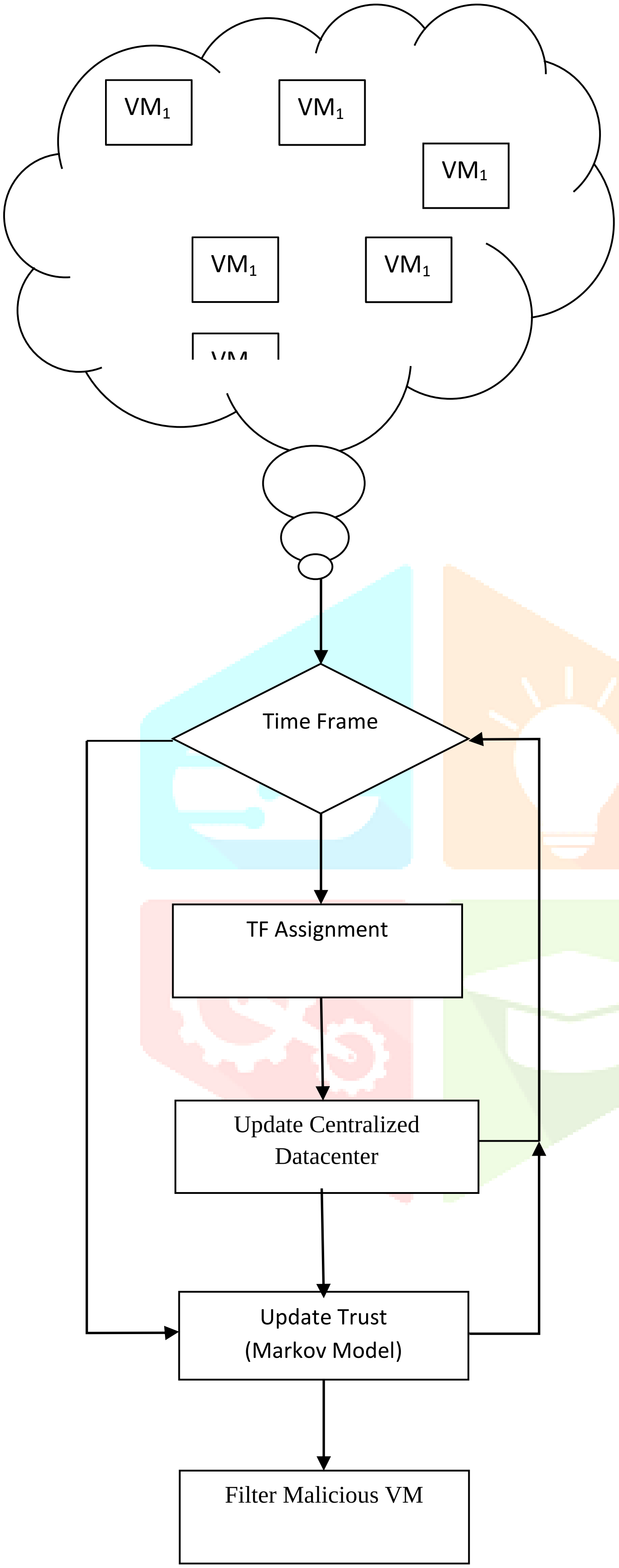

Fig.1 Proposed work training module.

(processor, memory, etc.), number of assignment initiated, number of assignment completed, VM Trust, Session between $VM_{i,j}$. Datacenter value get update at each instance of a time frame TF. While trust value get update after completion of TF. Time period of TF can be modify as per requirement.

Trust: It's a numeric feature of the virtual machine, range between 0 to 1. A VM having trust value 0 means VMS performance in the cloud was very poor with other VM in the cloud. Similarly if a VM having trust value 1 means VMS performance in the cloud was excellent with other VM in the cloud. In this work VMS of VM were used to estimate T after TF. For a fresh VM, cloud assign a Td value range between (0.3 to 0.6).

Table 1 Notation used in paper.

Notation	Meaning
VM	Virtual Machine
CDC	Centralized Datacenter
TF	Time Frame
VMS	VM Session
T	Trust
T_d	Trust Default Value
n	Number of VM in Cloud

Develop Cloud

In order to start the work some of VM were need to set in the cloud. CDC matrix should be initlized by null. Ssimilary trust of each machine were also assign by a default value T_d. TF value is an integer counter range {20, 25, 35,……..100}. Very small TF value or very large TF value leads to imbalance the model, so range will work properly. TF duration VMS were stored at each instance in the relevant matrix of CDC, this information was utilized for the trust calculation.

Markov Model

Pattern were evaluate in the markov model and cunt of those patterns in the dataset was used to evaluate support value in the model. Second order markov model was known for two element patterns in the dataset. Similarly third order markov model was known for three element patterns in the dataset. As cloud assign session between two VM, so second order model was proposed by the work for trust evaluation.

So if s number of VMS occurs between Vm$_i$ and VM$_j$ during tth time frame TF$_t$. Hence second order markov value SOM$_{i,j}$ between i and j. CDC maintain data of VMS in number of assignment initiated, number of session completed matrix MSC, Session between VM$_{i,j}$ Matrix MS.

$$Total\_Sessioni_{i,j} = MS(i,j) \text{ ---------Eq. 1}$$

$$Total\_Sessioni\_Complete_{i,j} = MSC(i,j) \text{ ---------Eq. 2}$$

$$SOM_{i,j} = \frac{Total\_Sessioni\_Complete_{i,j}}{Total\_Sessioni_{i,j}} \text{---------Eq. 3}$$

So as per markov model presentation i→j pattern have support value of $SOM_{i,j}$

Based on this i may have n number of support value one for each machine in the cloud if have done any assignment. So a single value need to calculate as per the estimation ofmarkov support.

$$TM_i = 1 - \frac{1}{\sum_{j=1}^{n} SOM_{i,j}} \text{---------Eq. 4}$$

This can be understand by an example Let a cloud have 4 machine and MS matrix looks like:

MS=

VM	1	2	3	4
1	0	4	2	7
2	3	0	4	3
3	4	5	0	0
4	1	0	9	0

Similarly MSC matrix have complete session count:

MSC=

VM	1	2	3	4
1	0	3	2	5
2	3	0	1	3
3	2	3	0	0
4	1	0	7	0

So trust of VM 1 is evaluate by second order markov model using eq. 1 and 2 is

SOM=

VM		Support
1	2	3/4=0.75
1	3	2/2=1
1	4	5/7=0.7142

So finally trust of each node was estimate by eq. 4

TM=

VM	Support
1	1-(1/2.4642) =0.594
2	1-(1/2.25) =0.55
3	1-(1/0.8) =0.09
4	1-(1/1.778) =0.4375

It was shown from above calculation that VM which perform good behavior with other VM in the cloud have higher trust count as VM1 have highest trust value as most of assignment was complete by the VM1. While VM3 has lowest trust value as incomplete behavior was done in the cloud. This help to detect the different type of attack work in the network perfrom by various malicious machine.

IV. Experiment and results

Experimental Setup: MATLAB platform was used in the work for implementation of cloud environment. This work has performed experiment under gray, and denial of service attack. Proposed model was implemented on 4GB RAM, i3 processor having 6th generation. Proposed model was apply on 100 virtual machine and performed 14500 assignment.

Result

Results were evaluate under two type of condition first was no-attack condition and other was attack condition. In attack condition first was gray hole attack environment and other was denial of service attack.

No-attack Condition

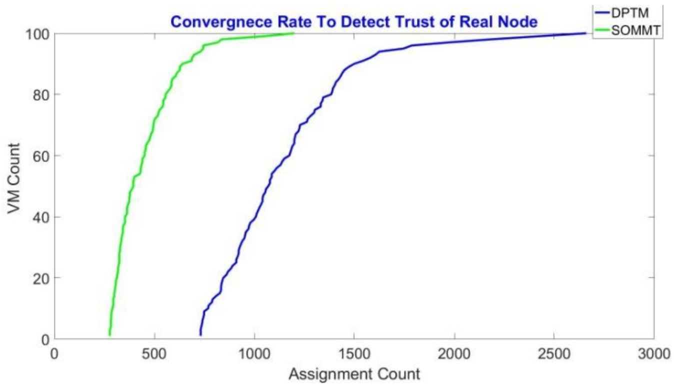

Fig. 2 Convergence detection rate in No-attack condition.

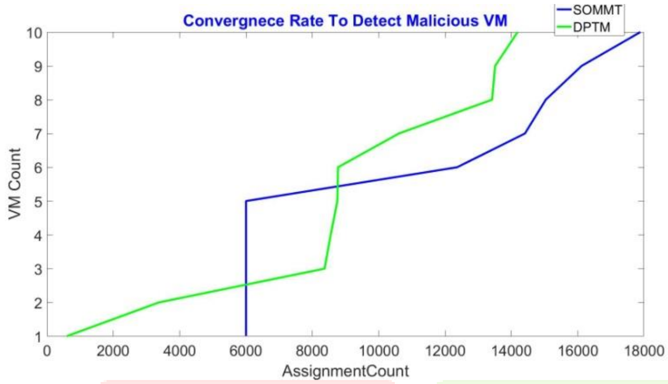

Fig. 3 Convergence detection rate in Grey-attack condition.

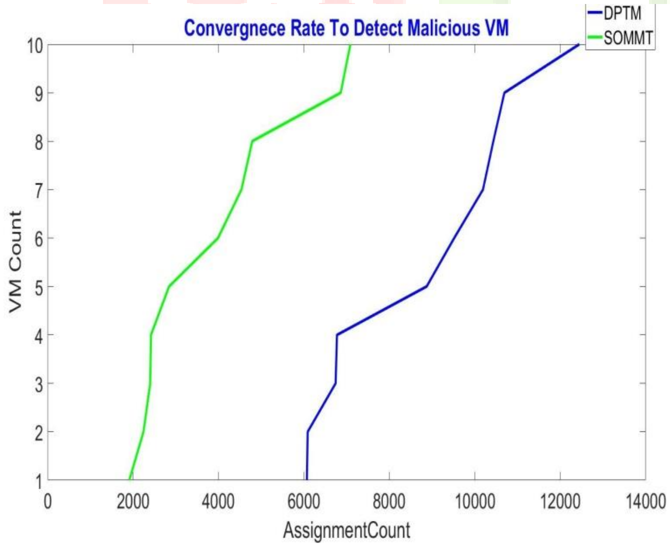

Fig. 4 Convergence detection rate in DOS-attack condition.

Above fig. 1 shows that all 100 real VM were detected by both the comparing algorithm in the cloud. But proposed model has increases trust value of all real VM in less number of assignment as compared to previous model in [2]. Similarly fig. 3, 4 shows that proposed model decreases the trust value of malicious VM and detect all 10 malicious VM in less number of assignment as compared to DPTM [2].

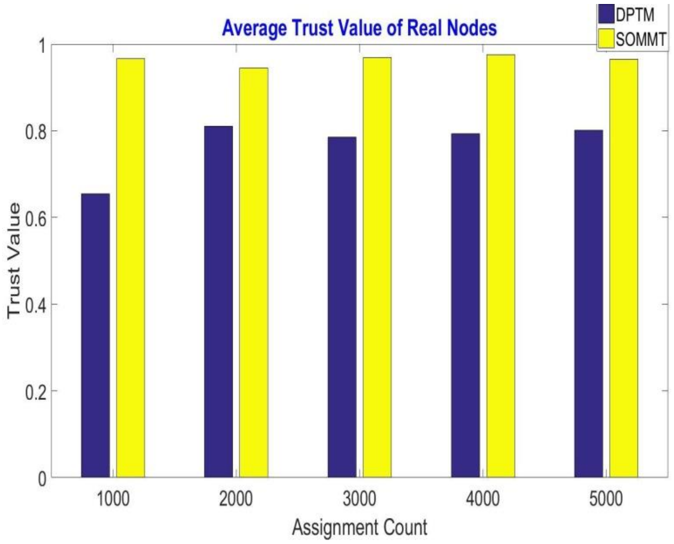

Fig. 5 Average convergence detection rate in No-attack condition.

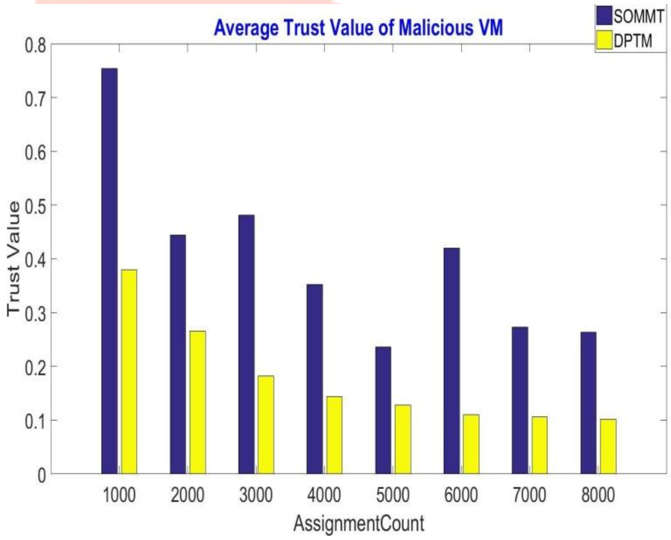

Fig. 6 Average convergence detection rate in grey attack condition.

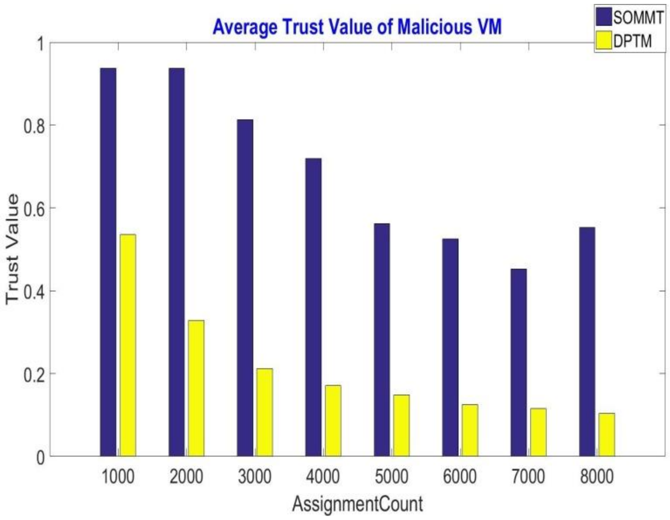

Fig. 7 Average convergence detection rate in No-attack condition.

Above graph shows that proposed SOMMT model has increase the trust value of real node in less number of assignment as compared to previous model [2]. Fig. 6 and 7 shows that proposed SOMMT model has reduced the trust value of malicious VM in cloud attacked environment in less number of assignment as compared to DPTM in [2]. Use of markov model for trust value calculation after fix time frame has increases this detection accuracy.

V. CONCLUSIONS

Intruder in any cloud is a curse for operation, resources, etc. So detection of such machines in less time is always a task for cloud computing researcher. This work has proposed a trust evalutionmodel for the virtual machine behavior analysis. Trust was estimate after fix time interval for each node, as per cumulative feedback of other VM in cloud, by second order markov model. Experiment was doen in no –attack and attack envrionemnt. Result shows that all 100 real VM were detected by both the comparing algorithm in the cloud. But proposed SOMMT model has increases trust value of all real VM in less number of assignment as compared to previous model in [2]. Similarly it was also found that proposed SOMMT model decreases the trust value of malicious VM and detect all 10 malicious VM in less number of assignment as compared to DPTM [2].

References

[1] V. Sulochana and R. Parimelazhagan, “A Puzzle Based Authentication Scheme for Cloud Computing,” International Journal of Computer Trends and Technology (IJCTT), Vol. 6, Issue 4, pp. 210-213, Dec. 2013.

[2] 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, VOL. 13, NO. 9, SEPTEMBER 2018.

[3] Azad M.A., Bag S., Hao F., Salah K. M2m-rep: Reputation system for machines in the internet of things. Comput. Secur. 2018.

[4] 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 April 2016; pp. 1–8.

[5] 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;29:694–706.

[6] Aluvalu, RK, Muddana, L. A survey on access control models in cloud computing. India: Springer, 2015. Emerging ICT for Bridging the Future.

[7] Rohit, R, Bharat, B. EPICS: a framework for enforcing security policies in composite web services. IEEE Trans Serv Comput 2019.

[8] Bhatia, R, Singh, M. A novel trust-based privacy preserving access control framework in web services paradigm. Adv Intell Syst, Adv Intel Syst Comput 2015; 308: 441–453.

[9] Nogoorani, SD, Jalili, R. TIRIAC: a trust-driven risk-aware access control framework for Grid environments. Future Gener Comp Sys 2016; 55: 238–254.

[10] Matin, C, Nima, JN. A new method for trust and reputation evaluation in the cloud environments using

the recommendations of opinion leaders' entities and removing the effect of troll entities. Comput Hum Behav 2016; 60: 280–292.

[11] P. Zhang, Y. Kong and M. Zhou, "A Domain Partition-Based Trust Model for Unreliable Clouds," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2167-2178, Sept. 2018.

[12] J. Liang, M. Zhang and V. C. M. Leung, "A Reliable Trust Computing Mechanism Based on Multisource Feedback and Fog Computing in Social Sensor Cloud," in *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5481-5490, June 2020.

[13] T. Wang, H. Luo, W. Jia, A. Liu and M. Xie, "MTES: An Intelligent Trust Evaluation Scheme in Sensor-Cloud-Enabled Industrial Internet of Things," in *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2054-2062, March 2020.