Pragya Richhariya, 2021, 9:4
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

A Survey on Cloud Virtual Machine Management Techniques and Features

Pragya Richhariya, Dr. Shailja Sharma
Computer Science and Engineering
Rabinadranath Tagore University
Bhopal MP India

Abstract- Cloud gives flexibility to many industries either related to product or services. This flexibility indirectly invites various types of attack on the system. Attacks may increases data losses, load, delay in services etc. So security of cloud management depends on attack detection algorithms. This paper has summarized various cloud security work proposed by scholars that uses trust management. Paper has brief trust calculation techniques adopt by researcher in previous years to identify malicious node in the network. Evaluation parameters were also detail by the work for the trust method comparison.

Keywords: Cloud computing, Trust management, Cloud Security.

I. INTRODUCTION

With the rapid development of computer communication technology (production, life, etc.). The size of the computer network is rapidly expanding. Cloud computing connects large-scale computing resources and storage resources through the network with effective integration that will provide reliable (cheap (convenient) services to users [1].

The tenant reduces the user's hardware resources software license and system maintenance. The investment cost of protection & but the high performance and low cost of cloud computing are excellent. The trend has also attracted the attention of cybercriminals.

In addition, the tenant identity verification is not Strict (increased security vulnerabilities and other factors, more and more attackers are attacking them. The source of the attack is moved to the cloud to expand its attack capability and attack range. The security alliance regards the phenomenon of cloud service abuse as the first problem facing cloud computing. The main focus is on protecting data in the cloud and cloud tenants from attacks outside the cloud [2].

However, there is little attention to the abuse of cloud services in aspects such as human intrusion and so on. This believes that the cloud service provider should deal with malicious programs located on it. Have the ability to identify (control and hold accountable) prevent yourself from becoming evil on the Internet.

The security problems faced by big computer networks have gradually become a major issue. Many portals are therefore subject to severe Heavy economic loss and ordinary users are also caused by the attack, as the network is down. DDoS attack has destruct approx 70 different services of the internet including Paypal, Github, Amazon, and Twitter was brought down recently due to a destructive and malicious DDoS attack. Now the attackers have taken the benefits of cloud computing and IOT technologies to generate heavy traffic of over 665 GB/s. [3, 4]

The attack research work merely focuses on detecting, filtering, source tracking of the attackers, and several other protection methods.

The DDoS attack has increased rapidly these days especially now when the cloud detection of malicious machines is complex due to the flexible environment and vulnerability in the cloud computing environment [5].

The data-based which is based on DDoS intrusion detection is found to be old as it lacks to predict the

pattern of dynamic changes in the cloud environment due to its constant pattern[6,7]. So there was a need to develop a new model to recognize the malicious activity in such changing environment.

II. TRUST-BASED MODELS

1. FIFO Model:
It comes under the categorization of the non-trusted model. In this model, list of potential cloud resources for a particular user QoS requirement is identified and a job is allocated to the first cloud resource [4].

2. QoS Trust Model:
It falls under the category of trusted‧ models by Paul Manuel. Quality of Service (QoS) is based on the attributes such as availability, reliability, data integrity and turn around efficiency. It works according to following equation [3], in which Cloud resource with the highest value is selected for the job [4].

3. Combined Trust Model:
In this architecture of trust models – three models named as Capability, Identity and Behavior - based Trust. In this framework, a job is proposed to the cloud resource selected. The decision is based on the three attributes. SLA Based Trust Model: In these model two inputs such as service level agreements criteria and experiences of users are used to test the level of trustworthiness for resources used in the cloud. The main characteristics of this model are that it can be implemented for different domains of cloud services and based on those domain users are able to obtain particular trust value of the same type of services [5].

4. Trust model for a file Exchange:
In Canedo, E. D., de Sousa Junior Et. al proposed a trust model for a file exchange in a secure and reliable manner. This trust model focuses on computational problems in an area related to security, trust, and reputation to ensure exchange of files on private cloud [6].

5. Interaction based Trust model:
Ahmad et al. propose a trust model based an interaction between the cloud provider and user [7]. This model works in three turns the first turn consists of satisfaction level of the user for previous experience of a cloud provider. In the second turn, the user must have concerns about cloud computing issues such as SLA, cloud advantages and disadvantages related to securities at different levels. Second turn emphasis on implementation of different securities cloud provider can be assumed to be reliable. At the third turn, a user can trust on the reliable cloud provider.

6. Trust Evaluation Model:
Xiaonian Wu et al. proposes a trust evaluation model based on D-S evidence theory and sliding windows for the evaluation of the credibility of the entities and detect the malicious entities[8]. In this architecture of trust model first-hand evidence is interaction among entities and sliding window is used to evaluate the timeliness of interaction evidence. Trust is calculated on the basis of D-S theory with help of interaction devices.

7. Turnaround trust Model:
In this trust model cloud resources will be selected according to the two factors such as trust and run-speed. Further, trust is a composition of availability, reliability and data integrity and turnaround efficiency. It works according to the following equations, which are used to calculate the values [9].

8. Behavior-Based Trust Model:
In these types of models system follows the user behavior transactions history to judge the behavior and privacy of grid entities, it is also helpful to protect cloud resources and cloud-based application. This model dynamically judges the security levels of the cloud-based services and due to this mechanism, the service provider can easily detect the user behaviors so they can easily fulfill the security-related requirements [4].

9. TVEM Based Trust Model:
Trusted Virtual‧ Environment Module (TVEM) is trust- based module software which provides trust-based services to a virtual environment of cloud-based services [10]. This module is a protection module and plays a vital role in the trust for a virtual environment which can be situated at any remote location and the virtual machine environment has the migration based possibilities to other platforms. The only downside point of TVEM is it cannot be implemented in hardware; we can only implement this trust-based module in software. The reason behind this is TVEM is software, which is working based on the phenomena of Trust base data module and cryptographic confidentiality module.

III. LITERATURE SURVEY

Bharot et al. in [11] proposed a feature selection method using a mitigation model that contains ICRPU or Intensive Care Request Processing Unit combined with J 48 algorithm. I

n the work, the Helliger distance function was used to determine the traffic. The benefit of using the ICRPU technique was that through this the attackers will never come to know that the request they have to send to destroy the resources are being captured and so they will not perform any further steps to override it. Thus it will become easy to locate and monitor the activity of the attacker.

Pallavi et. al. in [12] A multi-tenant database management was developed named SEMTDBMS especially for the cloud computing environment. It first analyzes the security parameters in terms of the secureness weight metric of the tenant workers and then a novel workload scheduler among the remaining tenants is being established.

Hyunjin Kim et. al. in [13] given an intelligent application to determine the abnormal behavior in the V2C environment based on image-based technique which was supported by AI or ISRM-AI to improve the service security of the cloud vehicle. System information such as memory on V2c, CPU, and network was generated by this ISRM-AI. The system was also effective to determine CNN or convolution neural networks in case of detection of any abnormal behavior in the network. A service environment was made to check the performance of this proposed system.

Saxena et. al. in [14], given TPA or a third-party auditor which was based on a packet trace back system. The given method utilizes Weibull distribution to predict the source of the attack (DDoS).

The approach proved to e effective in predicting genuine identification which was dependent on the flaws that the attackers have left. The traffic pattern of the various attackers was studied indifferent cloud environment. Reduced load in the cloud environment was one of the advantages of using this approach. Reliability, availability, and the median life of DDos can easily be determined with the help of Weibull distribution.

Omar Abdel Wahab et. al. in [15] given a two-way solution by which a trust relationship can be developed within the virtual guest machines by providing the objective and subjective resources which was then employed and combined with an interface called as "Bayesian interface".

A game was designed among all the participants or hypervisors that try to control the inadequate budget of the resources and maximize the minimization that was done by DDoS attackers. In this game, the hypervisor can control the load distribution among VMs in real-time to detect the DDoS attackers.

Subramanian1 et. Al. in [16] shape the future generation of cloud security using convolution neural network because CNN can provide automatic and responsive approaches to enhance security in cloud environment. Instead of focusing only on detecting and identifying sensitive data patterns, ML can provide solutions which incorporate holistic algorithms for secure enterprise data throughout all the cloud applications.

Zina et. Al in [17], proposed two models for intrusion detection and classification scheme Trust-based intrusion detection and classification system (TIDCS) and trust-based intrusion detection and classification system- accelerated (TIDCS-A) for secure network. TIDCS reduces the number of features in the input data based on a new algorithm for feature selection. Initially, the features are grouped randomly to increase the probability of making them participating in the generation of different groups, and sorted based on their accuracy scores.

Only the high ranked features are then selected to obtain a classification for any received packet from the nodes in the network, which is saved as part of the node's past performance.

TIDCS proposes a periodic system cleansing where trust relationships between participant nodes are evaluated and renewed periodically. TIDCS-A proposes a dynamic algorithm to compute the exact time for nodes cleansing states and restricts the exposure window of the nodes.

The final classification decision for both models is estimated by incorporating the nodes past behavior with the machine learning algorithm. Any detected

attack reduces the trustworthiness of the nodes involved, leading to a dynamic system cleansing.

III. ATTACKER TYPES AND RISKS

Many of the security threats and challenges in cloud computing will be familiar to organizations managing in house infrastructure and those involved in traditional outsourcing models. Each of the cloud computing service delivery models' threats result from the attackers that can be divided into two groups [18].

1. Internal Attackers:

- Is employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service
- May have existing authorized access to cloud services, customer data or supporting infrastructure and applications, depending on their organizational role
- Uses existing privileges to gain further access or support third parties in executing attacks against the confidentiality integrity and availability of information within the cloud service.

2. External Attackers:

- Is not employed by the cloud service provider, customer or other third party provider organization supporting the operation of a cloud service.
- Has no authorized access to cloud services, customer data or supporting infrastructure and applications
- Exploits technical, operational, process and social engineering vulnerabilities to attack a cloud service provider, customer or third party supporting organization to gain further access to propagate attacks against the confidentiality, integrity and availability of information within the cloud service.

3. Cloud Security Risks:

The security risks associated with each cloud delivery model vary and are dependent on a wide range of factors including the sensitivity of information assets, cloud architectures and security control involved in a particular cloud environment. In the following we discuss these risks in a general context, except where a specific reference to the cloud delivery model is made [18].

3.1 Privileged user access: Cloud providers generally have unlimited access to user data, controls are needed to address the risk of privileged user access leading to compromised customer data.

3.2 Data location and segregation: Customers may not know where their data is being stored and there may be a risk of data being stored alongside other customers' information.

3.3 Data disposal: Cloud data deletion and disposal is a risk, particularly where hardware is dynamically issued to customers based on their needs. The risk of data not being deleted from data stores, backups and physical media during decommissioning is enhanced within the cloud.

3.4 E-investigations and Protective monitoring: The ability for cloud customers to invoke their own electronic investigations procedures within the cloud can be limited by the delivery model in use, and the access and complexity of the cloud architecture. Customers cannot effectively deploy monitoring systems on infrastructure they do not own; they must rely on the systems in use by the cloud service provider to support investigations.

3.5 Assuring cloud security: Customers cannot easily assure the security of systems that they do not directly control without using SLAs and having the right to audit security controls within their agreements.

V. EVALUATION PARAMETERS

In order to compare various methods of malicious node detection in cloud environment, evaluation parameters were used. This section of paper discusses few of these parameters with evaluation formulas.

	Compare Algorithm	
Actual	T (Real)	F (Malicious)
P (Real)	TP	FP
N (Malicious)	TN	FN

1. TP is true positive counter:

This counter increases when model identify correct (Real) class of cloud node and actual class of node is also real.

2. FP is false positive counter:

This counter increases when model identify malicious class of cloud node and actual class of node is real.

Similarly other counter increases accordingly.

$$Precision = \frac{TP}{TP+FP}$$-------Eq. 1

$$Recall = \frac{TP}{TP+FN}$$-------Eq. 2

$$FMeasure = \frac{2*Precision*Recall}{Precision+Re}$$-------Eq. 3

$$Accuracy = \frac{TP+TN}{TP+TN+FP+F}$$-------Eq. 4

3. Execution Time:

This parameter is to evaluate execution time of the algorithm that is time taken by the proposed method for execution. Algorithm time is expected after the evaluation of the real and malicious class.

VI. CONCLUSION

Cloud working depends on virtual machine, so management of such unknown computers need close monitoring. Many of virtual machine are working to increase load on cloud and reduce its efficiency. This paper has survey on different techniques proposed by scholars of cloud virtual machine management. It was obtained that trust based cloud management is efficient and more robust against intruders. Hence paper has summarized different type of trust management schemes adopt or proposed by researcher. Various types of risk associate with cloud in form of attacks were also list by the paper. In future scholar can developed a model that can prevent or generate alarm, against any attack by using machine learning techniques.

REFERENCES

[1] Priya .G, Jaisankar N, "A Reputation Based Trustworthy System For Cloud Environment" in International Journal of pharmacy and Technology, Vol 8, No. 3, pp No:16702-16708, September 2016.

[2] Piyush Kumar Jain, Prof. Rupali Bhartiya . "GASBE: A Graded Attribute-Based Solution for Access Control in Cloud Computing". Volume-7, issue 4, 2021.

[3] Ashish Gupta, Akhilesh Bansiya. "A Review on Block Chain in Cloud Computing Healthcare Data Security". Volume 8, issue 4, 2020.

[4] P. Manuel, "A trust model of cloud computing based on Quality of Service", Annals of Operations Research, Vol.233, Issue.1, pp. 281-292, 2015.

[5] M. Alhamad, T. Dillon, "SLA-Based Trust Model for Cloud Computing", In the proceedings of the 13th International Conference on Network-Based Information Systems, Japan , pp. 321-324, 2010.

[6] E. D. Canedo, R. T. Junior, "File Exchange in a Private Cloud supported by a Trust Model" , In the proceedings of the 2012 International conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, China, pp. 89-96, 2012.

[7] S.Ahmad, B. Ahmad, S. M. Saqib, R. M. Khattak, "Trust model: Cloud's provider and cloud's user", International Journal of Advanced Science and Technology, Vol.44, pp. 69-80, 2012.

[8] X. Wu, R. Zhang, B. Zeng, S. Zhou, "A trust evaluation model for cloud computing", Procedia Computer Science, Vol.17, pp.1170-1177, 2013.

[9] A. Gholami, M. G. Arani, "A trust model based on quality of service in cloud computing environment", International Journal of Database Theory and Application, Vol. 8, Issue.5, pp.161-170, 2015.

[10] F. J. Krautheim, D. S. Phatak, A. T. Sherman, "Introducing the Trusted Virtual Environment Module: A New Mechanism for Rooting Trust in Computing", In the proceedings of the International Conference on Trust and Trustworthy Computing, Germany, pp. 211– 227, 2010.

[11] Nitesh Bharot, Priyanka Verma, Sangeeta Sharma, Veenadhari Suraparaju. "Distributed denial-of-service attack detection and mitigation using feature selection and intensive care request processing unit". Proc. Comput. Eng. Comput. Sci., Arab. J. Sci. Eng., 2018.

[12] Pallavi, G.B., Jayarekha, P. Secure and efficient multi-tenant database management system for cloud computing environment. Int. j. inf. tecnol. (2020).

[13] Hyunjin Kim, Sang Hong, Jinsul Kim, And Jaecheol Ryou "Intelligent Application Protection Mechanism for Transportation in V2C Environment". Special Section on Big Data Technology and Applications in Intelligent Transportation May 20, 2020.

[14] Saxena, R., Dey, S. DDoS attack prevention using collaborative approach for cloud computing. Cluster Comput 23, 1329–1344 2020.

[15] Omar Abdel Wahab, Jamal Bentahar, Hadi Otrok, and Azzam Mourad. "Optimal Load Distribution for the Detection of VM-based DDoS Attacks in the Cloud". IEEE Transaction, Services Computing Nov. 2020.

[16] E. K. Subramanian, LathaTamilselvan. "A focus on future cloud: machine learning-based cloud security". Service Oriented Computing and Applications, 12 August 2019.

[17] Zina Chkirbene, AimanErbad, RidhaHamila, Amr Mohamed, Mohsen Guizani, and Mounir Hamdi. "TIDCS: A Dynamic Intrusion Detection and Classification System Based Feature Selection". Digital Object Identifier June 3, 2020.

[18] Security and Security and Privacy Privacy Issues in Cloud Computing Jaydip Sen Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.