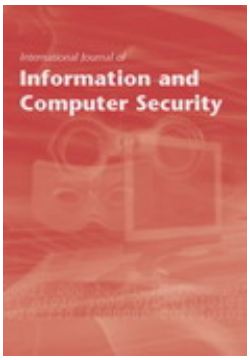


International Journal of Information and Computer Security

ISSN online: 1744-1773 - ISSN print: 1744-1765
https://www.inderscience.com/ijics

Priority-based security-aware virtual machine allocation policy

Aparna Bhonde, Satish R. Devane

DOI: 10.1504/IJICS.2023.10057700

Article History:

Received:	26 September 2022
Last revised:	07 March 2023
Accepted:	20 March 2023
Published online:	19 February 2024

Priority-based security-aware virtual machine allocation policy

Aparna Bhonde* and Satish R. Devane

Computer Science,
Datta Meghe College of Engineering,
Mumbai University,
Sec 3, Airoli, Navi Mumbai,
400708, Maharashtra, India
Email: aparna.bhonde@dmce.ac.in
Email: satish.devane@dmce.ac.in
*Corresponding author

Abstract: Rapid expansion of cloud computing raises several issues, including loss of quality of service (QoS) due to resource sharing and increased security concerns to virtual machines (VMs) resulting from co-residency with other vulnerable VMs on the same physical machine (PM). However, due to lack of reliable security metrics and consolidation of VMs without awareness of security risk, cloud datacentre's threat score increases. We present a priority-based secure virtual machine allocation policy that calculates five-dimensional threat score and lowers the overall datacentre threat score after prioritising the threat score based on attack surface which reduces average value by 9% and maximum of 18% when compared with power aware best fit decreasing (PABFD) policy with maximum increase of 4% in energy consumption at priority (0.5, 0.3, 0.2) for network, VMM along with hosted VM's and PM respectively. The comparative analysis with similar security-based studies assures to deliver better service quality.

Keywords: virtual machine placement policy; coresidency; quality of service; datacentre threat score; threat assessment model.

Reference to this paper should be made as follows: Bhonde, A. and Devane, S.R. (2024) 'Priority-based security-aware virtual machine allocation policy', *Int. J. Information and Computer Security*, Vol. 23, No. 1, pp.40–56.

Biographical notes: Aparna Bhonde is a research scholar and working as a faculty in reputed Engineering College in Mumbai, India since 15 years. She has completed her Master's of Information Technology from Mumbai University. Her research interests include cloud security, network security, and IoT.

Satish R. Devane is a Professor in a reputed Engineering College in Mumbai, India and having experience of 34 years. He completed his PhD from the Indian Institute of Technology Bombay (IITB). He is working in an advisory boards of many engineering colleges in India.

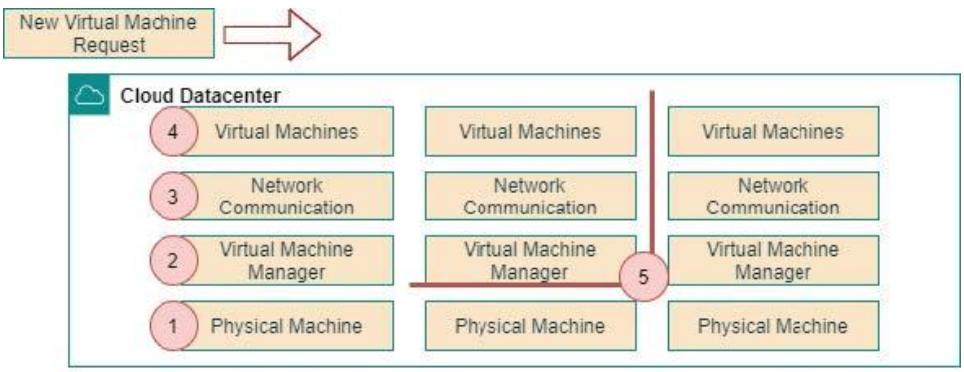
1 Introduction

The shift to cloud computing has improved the efficiency of virtual work places and the provision of digital services. More businesses will adopt virtual workplaces in the upcoming years, utilising a variety of services (Goasduff and Stamford, 2021) Pay per use, on-demand features enable firms to outsource a portion of their operations on cloud in order to speed up services and increase value. Despite the fact that many different factors influence security, cloud computing technologies like virtualisation and multitenancy, along with their on-demand features, open up new security entry points for malicious actions (Parast et al., 2022). Recent studies have concentrated on virtual machine consolidation as a viable solution to address energy consumption issues in cloud datacentres without going against service level agreements (Escheikh et al., 2018) nevertheless, the detrimental effects of VM consolidation on security have received little attention. With the adoption of multitenancy in cloud computing, computers from diverse businesses are situated close to one another and granted access to shared memory and resources, resulting in a new attack surface (RA, 2016). In order to construct secure higher-level clouds, having a locked IaaS cloud is a requirement. IAAS level attacks on VMs, VMMs, or networks are conceivable as a result of the multitenancy environment (Vaquero et al., 2011). The usage of virtualisation enables third party cloud providers to multiplex several client VMs across a shared physical infrastructure in order to maximise the utilisation of existing capital expenses. Co-resident attacks are reported to be viable due to shared resources that result in information gain (Ristenpart et al., 2009). The VM allocation policy is crucial in preventing co-residency attacks. Cloud security is impacted by the placement of VMs in the cloud datacentre, which also has a significant impact on QoS. While spinning the VM request there is a need to consider the threats associated with the datacentre to avoid the possibility of attacks due to co-residency.

In this paper, we propose the novel priority-based secure virtual machine placement algorithm based on 5-dimensional threats along with related attack surface priorities associated with VMs in datacentres. Appropriate host is mapped to the new VM instance after threat score is calculated. We have considered the datacentre components present at the IAAS level which help to spin a new VM instance in the datacentre. We propose an algorithm for VM placement that will consider the threats at different levels as shown in Figure 1 and accordingly select the host from the datacentre. The threats assessment metrics considers threats which are based on vulnerability score and are associated with the VM image, the VMM used to create VM instances, the other co-located VMs on the specific VMM, network vulnerability associated with direct paths and common services, and the vulnerability score for PMs, which provides the overall datacentre threat score (ODTS). Attacks originating from VMs and leading to side channel attacks are studied and classified. Based on classification, priorities are decided for the threat scores. The algorithm helps to select the appropriate host from the cloud datacentre which bounds the ODTS to remain low. Even after placing the new VM request in the cloud datacentre, the ODTS does not exceed the mean of the ODTS. In this way, the ODTS does not have a significant change and helps to keep the security intact. Every time the new VM instance is ready for spinning, the new ODTS is calculated hence there is continuous monitoring of the datacentre threats while placing the new VM instance. We have considered the initial placement of the new VM on the basis of ODTS and utilisation, hence avoiding the need for immediate migration.

We have used cloud-sim to evaluate the algorithm. Cloud-sim is a well-known and dependable cloud simulator however, we have done significant modifications to calculate and accept the threat scores for the datacentre. After a few modifications, we have compared our algorithm with the power-aware best fit decreasing (PABFD) which is default VM selection algorithm available in cloud-sim. The work is also compared with similar studies on basis of threat score.

Figure 1 Datacentre threat assessment metrics (see online version for colours)



Simulation results show that the VMs placed by priority-based secure virtual machine allocation policy show elevated security enhancements by keeping the overall datacentre threat score below the mean value and limits the overall datacentre threat score resulting in reduced average value by 9% and maximum of 18% when compared with power aware best fit decreasing (PABFD) policy having the maximum increase of 4% in energy consumption when the priority are set to (0.5, 0.3, 0.2) for the network, VMM along with hosted VM's and PM respectively. This enhances cloud security and assures to deliver better service quality.

Rest of the paper is organised as follows: Section 2 represents the related work. In Section 3, our methodology is explained. Next in Section 4, simulation results are explained and Section 5 covers the conclusion and future scope.

2 Related work

Virtual machine placement is a critical operation that is conducted to determine the most appropriate PM or server to host the VM. Selecting a suitable host is very important to improve power efficiency, resource utilisation, and QoS support in a cloud computing environment. It is difficult to find the optimal solution for placing the VM in a large datacentre with unpredictable VM requests and load is shown to be an NP-hard problem. Host underload detection, host overload detection, VM selection, and VM placement are the four phases that make up the VM placement policy. While considering the VM placement, objectives like resource-aware, cost-aware, power-aware, network-aware, and performance-aware policies are considered ignoring the impact of such placements on the co-residence security of the virtual machines. Many attempts have been done to reduce the co-residency, Based on VM placement, authors in sought to reduce the hazards associated with the multi-user environment. According to Afoulki et al. (2011)

suggestion, a list of users who should not be assigned to the same host together based on users' opponents should be created. Knowing users and enemies is necessary for their strategy, which is challenging in public clouds.

Han et al. (2015) gave an approach that models to maximise the efficiency and coverage rates required for attackers to occupy as many servers as possible with the minimum number of VMs. This is achieved by placing the request on previously selected server first and if not found than select the server with least number of VM's hosted, however the drawback is from users' point of view, as the failure of one server will impact all the VMs of a user. Hasan and Rahman (2020) analyses the co-resident attacks and corresponding defence strategies, with respect to benign and malicious VMs and the defender, i.e., the VM monitor (VMM), using a signalling game model. The solutions to the game provide optimal defence strategies for the VMM with respect to the expected number of malicious VMs in collaboration. They evaluate the game results through simulations of various synthetic attack scenarios. The results show that the defender can effectively resist co-resident attacks by distinguishing the benign and malicious VMs. We have observed that some of the important parameters such as Poisson distributed process, maximum time bond for the information gain, cost is not considered which has higher chances to decrease the equilibrium results.

Gaggero and Caviglione (2018) proposed a holistic placement framework considering conflicting performance metrics, such as the service level delivered by the cloud, the energetic footprint, hardware or software outages, and security policy which devise optimal mapping between virtual and physical machines. It has proposed a framework to choose how to deploy VMs on PMs by pursuing conflicting performance goals, such as counteracting hardware outages or software aging issues, ensuring proper security policies, maintaining a suitable service level, and reducing power requirements. To compute the optimal strategies a method based on MPC is developed, which has allowed taking into account constraints while exploiting future information but security is addressed merely by grading the SLA for security.

Han et al. (2018) proposed a multi-objective method called security-ware multi-objective optimisation-based virtual machine placement algorithm (SMOOP). This algorithm considers three objectives to optimise that is security risk, resource waste and network traffic. One of the advantages of this method compared to others is that cloud providers can extend their objectives and define new constraints such as the migration cost or energy consumption, based on their preferences. Of course, a set of shortcomings still exist. For example, the hesitancy and uncertainty in the calculation of the aforementioned objectives have not been considered. Also, the priority of these objectives is another compelling point that is not reflected. Zhang et al. (2011) introduced HomeAlone, a system that lets a tenant verify its VMs' exclusive use of a physical machine. The key idea in HomeAlone is to invert the usual application of side channels. Rather than exploiting a side channel as a vector of attack, HomeAlone uses a side-channel (in the L2 memory cache) as a novel, defensive detection tool. By analysing cache usage during periods in which 'friendly' VMs coordinate to avoid portions of the cache, a tenant using HomeAlone can detect the activity of a co-resident 'foe' VM. It includes classification techniques to analyse cache usage and guest operating system kernel modifications that minimise the performance impact of friendly VMs sidestepping monitored cache portions.

In Feizollahibarough and Ashtiani (2021), the authors proposed a security-aware virtual machine placement scheme to reduce the risk of co-location for vulnerable virtual

machines. Four attributes are introduced to reduce the aforementioned risk including the vulnerability level of a virtual machine, the importance level of a virtual machine in the given context, the cumulative vulnerability level of a physical machine, and the capacity of a physical machine for the allocation of new virtual machines. Limited number of static attributes for risks is considered and the network risk calculated can be the need of any specific application which can be rated as false prediction as the problem is solved with fuzzy logic. Al-Haj et al. (2013) describe the formation of security groups on the basis of reachability requirements after calculating the virtual machines vulnerability score as well as virtual machines impact score and maps the placement.

Agarwal and Duong (2019) perform theoretical and empirical analysis of their algorithm previously co-located users first and creates co-location resistance for virtual machines. The algorithm chooses those physical machines which belong to the users who already have virtual machine instances hosted, in order to gain co-location near the existing instances. Azar et al. (2014) presented a random placement technique in which each PM in the data centre is dynamically designated as either OPEN (ready to accept more Vms), CLOSED (cannot accept more VMs), or EMPTY (do not host any VMs). A preset code parameter makes sure that PMs are always kept precisely OPEN. When a new VM request comes in, it is randomly assigned to PM Pjs from among OPEN PMs. To retain the precise number of PMs open, when Pj is full, it is tagged as CLOSED, and a PM identified as EMPTY is reclassified as OPEN. Deallocation of VMs is not covered by any policies. Yu et al. (2014) suggested a strategy for placement and migration based on Chinese wall policy. Relocation was suggested for the virtual machine based upon the isolation rules set upon the value of aggressive conflict of interest relation for every user. While this method has given appropriate rule sets for isolation, utilisation cost is not considered.

Our work focuses on the priority-based attack surfaces which are originating from the virtual machine in a cloud datacentre and gains co-location leading to various side channel attacks. We have considered all the datacentre components vulnerability mentioned in threat model. The selected priority values give the optimal solution satisfying security and energy consumption which is also important for cloud providers to reduce the carbon footprint.

3 Methodology

Threat assessment model calculates threat score and secure VM placement approach maps the VM instance to the physical machine. Datacentre consists of physical machines, virtual machine managers, network modes for direct communication and common services, VMs hosted on the virtual machine manager and virtual machine images. Attacker can compromise any of these component's vulnerabilities after gaining co-residency leading to stealing information and side channel attacks. To resist these attacks our approach calculates the threat score on the basis of vulnerability and maps the vm instance to physical machine. Our approach is also energy efficient along with security aspect that can be applied to cloud datacentres while VM consolidation. The approach limits the datacentre threat score which ensures the secure placement of virtual machines.

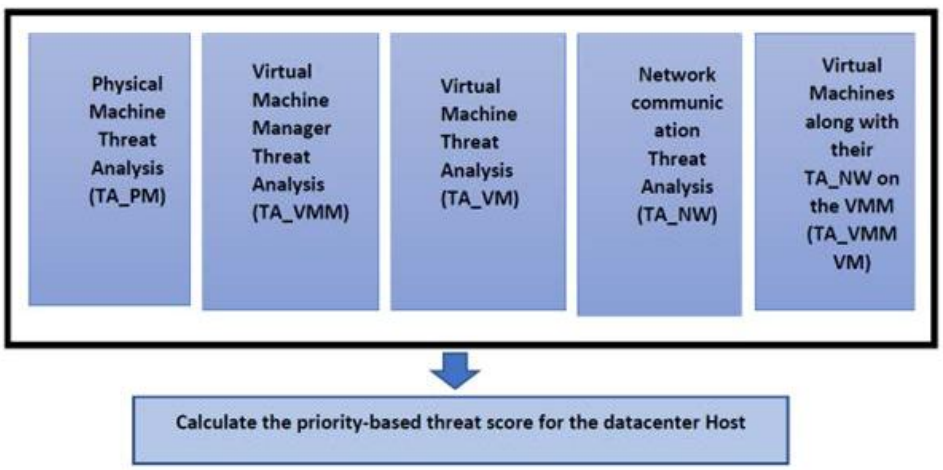
The threat assessment model calculates 5-dimensional threat score discussed below. Priorities of threats are considered on the basis of their impact while mounting the

co-residency attacks hence threat model considers threat priority α while calculating host threat score. The ODTS does not exceed the mean of the ODTS, even after spinning the new VM request to the cloud datacentre. With the security maintained in this way, there isnt any significant change to the datacentre threat score. To achieve the minimum ODTS we have used the threat assessment model and the algorithm which is discussed in Subsections 3.1 and 3.2.

3.1 Threat assessment model

The system uses a security-aware threat assessment model which prioritises the threats associated with the VM placement in the datacentre. Threat assessment model is responsible to consider vulnerabilities at various levels in the datacentre. Datacentre consists of physical machines, virtual machine managers, virtual machine images, network communication based on direct communication to the VMs on the same physical machines or different physical machines in the same datacentre, ports and network communication through common services. Figure 2 shows the block diagram for threat assessment model

Figure 2 Block diagram for threat assessment model (see online version for colours)



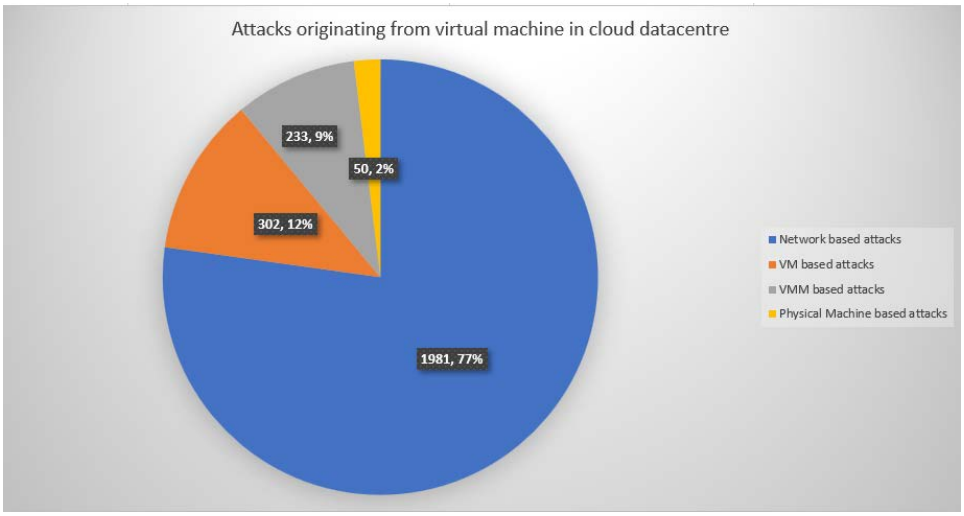
3.1.1 Prioritise the threat

Threats associated with datacentre from the above mentioned model have different impact which depends upon the severity of vulnerability and difficulty to exploit the vulnerability. Earlier survey has shown that virtual machines have the maximum attack surface on infrastructure as a service leading to violation of service level agreements. It is observed that virtual machine is used more than 80% as attack source. These findings have given the direction to study impact of cloud attacks on various components required to create and run VMs in a cloud datacentre. Past studies in Table 1 mention the types of attacks, its common vulnerability score count, its severity. Literature shows the various techniques followed by attackers to have the stated impact. The summary of survey is depicted in Table 1.

Table 1 Attacks originating from virtual machine in cloud datacentre

Types of attacks	*CVE count*	*Severity*	*Techniques used*	*Impact*
Network-based attacks (Mell et al., 2007; OWASP, 2022; Lin and Lee, 2012)	1981	High and critical	Port scanning	Distributed port scanning, denial of service
			Botnets	Botnet using Amazon cloud as command and control server
			Spoofing sttacks	ARP spoofing by VM
VM-based attacks (Liu et al., 2014; Grobauer et al., 2010; Gruschka and Jensen, 2010; Zhou et al., 2013; Fernandez et al., 2013)	302	High and critical	Cross VM side channel attacks	Violation of data protection
			VM creation attacks	Violation of data protection
			VM scheduler-based attacks	Theft-of-service
			Timed scheduling using hypervisor theft-of-service	Theft-of-service
			VM replication	Violation of data protection
VMM-based attacks (Szefer and Lee, 2012; Zhou et al., 2013)	233	Medium and high	VM migration and rollback attacks	Violation of data protection, malicious manipulation of data (IaaS)
			VM image access and relocation with insecure hypervisor	Violation of data protection, denial-of-service
			VM escape and VM hopping to access information of other VMs and impact hypervisor execution	Violation of data protection, denial-of-service
			Communication for VM migration and memory access	Violation of dataprotection, denial-of-service
Physical machine-based attacks (Liu and Chen, 2011)	50	Low and medium	Vulnerabilities associated with latest servers	Misconfiguration at datacentres, vulnerability exploitaion, malware attacks

Figure 3 Various attacks originating from VM in cloud datacentre (see online version for colours)



We have summarised the coverage of attacks in Figure 3. which shows 77% coverage for network-based attacks, 21% for VMs along with VMM and 2% for physical machine attacks. Referring to above study network threats are considered to be the biggest security challenge as it can lead to various attacks (Bogdanoski et al., 2013) following the consolidated threats from VMM and VM's placed on the host. The physical machine threats are having the lowest weightage priority, because it is difficult to exploit physical machine vulnerabilities, attackers avoid choosing that route to infiltrate the target computer, however possibility of misconfiguration at the client side cannot be ruled out. Depending on this analysis, we have set $\alpha 1$, $\alpha 2$, and $\alpha 3$ as the priority giving the weights as $\alpha 1 > \alpha 2 > \alpha 3$ where $\alpha 1$ the weight given for the network threat, $\alpha 2$ is the weight given for the VMM along with the hosted VM's on it and $\alpha 3$ is for physical machine threat. In the experimentation we have run multiple triplets where $\alpha 1 > \alpha 2 > \alpha 3$ and decided to gave the maximum share of 50% to network threats even though our literature gave the 77% coverage due to significant difference in energy consumption explained in Figures 5 and 7 for (0.5, 0.3, 0.2) and (0.6, 0.25, 0.15) under results section. Efficient energy consumption is necessary along with security in view of cloud service providers to reduce the carbon footprint. However, it is worth mentioning that cloud service provider can define the priority values according to the client requirements and add security for additional cost.

3.1.2 Calculation of security threats

A common tool to assess the vulnerabilities of software or hardware is the CVSS (Maris and Wiles, 2019). To create the vulnerability list for each PM or VM, we can utilise vulnerability scanner tools like Nessus and Qualys. The CVSS score rates the severity of vulnerabilities on a scale between 0 and 10. If different tools are utilised to rate vulnerabilities, we can pick CVSS as our reference point to standardise all vulnerability

scores. Table 2 represents the standard qualitative severity rating scale considered for the CVSS scores. The threat analysis is briefed as below.

Table 2 Standard qualitative severity rating scale

VM_CVSS_Base_Score < = 3.9	Low threat analysis score
VM_CVSS_Base_Score > = 4.0 && VM_CVSS_Base_Score < = 6.9	Medium threat analysis score
VM_CVSS_Base_Score > = 7.0 && VM_CVSS_Base_Score < = 8.9	High threat analysis score
VM_CVSS_Base_Score > = 9.0 && VM_CVSS_Base_Score < = 10.0	Critical threat analysis score

3.1.2.1 Network threat analysis

If the attackers VM gets success in gaining the co-residency it may exploit the other VMs present on the host. Network threat analysis considers direct communication paths associated with virtual machines, port communication and the communication through common services. Increase in number of hops increases the attack complexity hence we are limiting scope of this study to direct paths. To calculate the host threat score in the datacentre, we consider the network threat associated with the virtual machines which are already hosted on a particular physical machine. Following assessment encompasses all potential attack routes in a cloud.

- direct communications paths established by the hosted VM within the host and to other hosts
- port communication under the particular virtual private network
- common services shared among the VM's for example web services and the database server, which can lead to various attacks.

So we give the network threat analysis score for a virtual machine in the datacentre as

$$TA_{NWVM} = \sum (NW_{(directpath)}, NW_{(port)}, NW_{(commonservices)}) \tag{1}$$

The network threat analysis for the new virtual machine request is be calculated by the direct paths. The VM will fall in any virtual private cloud and hence the open ports for communication will be known. Following equation states the network threat analysis score for the new VM.

$$TA_{NWVM} = \sum (NW_{(directpath)}, NW_{(port)}) \tag{2}$$

3.1.2.2 Threat analysis of all the virtual machines on the VMM

The threat assessment score for virtual machine monitor is considered by self vulnerability and the VM's hosted on that virtual machine monitor.

1 Virtual machine manager threat analysis (TA_VMM): This is a threat analysis where the vulnerabilities associated with the different VMM's offered by cloud service provider like Xen, and KVM, in the data centre are considered. To quantify the vulnerability of N types of VMM, lets consider the list of virtual machines managers in a datacentre $TAVMM_{DC}$ = {VMM1, VMM2, VMM3, …, VMMn}. Virtual machine manager threat analysis is given by where K is the virtual machine manager chosen for creating virtualisation. Vulnerability is calculated using scanning tools.

2 Virtual machine threat analysis: This is a dynamic threat analysis where the vulnerabilities associated with the image selected for different virtual machines are considered. Let us consider the various images provisioned by the cloud datacentre as VM_{DC}= {VM1, VM2, VM3, …, VMn} so the virtual machine threat analysis TA_{VM} is given by VM_K where K is the virtual machine image chosen by clients for creating new VM instance. Vulnerability is calculated by scanning the VM image repository in cloud datacentre.

3 Calculation of threat analysis of all the virtual machines on the VMM:

$$TA_{VMM_{VM}} = TA_{VMMK} + \left(\sum_{k=0}^{n} TA_{VMK}\right) \Big/ (Number\ of\ VM's\ \ on\ the\ VMM_K) \tag{3}$$

where TA_{VMK} is calculated and average is taken for all the virtual machines hosted on a particular virtual machine manager. $TA_{VMM_{VM}}$ is the consolidated virtual machines threat analysis score with respect to particular VMM. This consolidated score mentions the threat score from co-resident virtual machines on the host. This can be explained with a scenario that a VMM of type XEN is used for creating virtualisation environment and it has four VMs running on it, in that case TA_{VMMK} represents the vulnerability of XEN hypervisor and $\sum_{k=0}^{n} TA_{VMK}$ represents vulnerability score of four VMs.

3.1.2.3 Physical machine threat analysis

This is a static type of threat analysis where the vulnerabilities associated with the physical machines in the data centres are considered. To quantify the vulnerability of each physical machine in the data centre having *n* physical machines (PM) than PM = {PM1, PM2, PM3, …, PMn}. The threat analysis for physical machines in data centre TA_{PM} is given by, PM_K Where k is the physical machine serving as host in the datacentre.

3.1.2.4 Host threat analysis score

Datacentre host threat score TA_{HOST} is calculated by considering priorities as discussed in Subsection 3.1.1. as shown below:

$$TA_{HOST} = TA_{PM} * \alpha 3 + TA_{VMMVM} * \alpha 2 + TA_{NWPM} * \alpha 1 \tag{4}$$

where $\alpha 1$, $\alpha 2$ and $\alpha 3$ are the priority for network threat, virtual machine manager along with the VMs and the physical machine threats respectively.

3.2 Priority-based secure VM allocation policy

The proposed approach calculates the threat assessment score for all the hosts present in the datacentres as well as the threat score for the virtual machine. The admissible treat score for the entire datacentre should be less than the mean threat analysis host score which is given by the mean of TA_{HOST}

$$TA_{Permissible} = \sum_{k=0}^{n} TA_{HOSTk} \Big/ Number\ of\ available\ TA_{Host} \tag{5}$$

The host threat score should be lower than the permissible threat analysis score when it is chosen to host new VM requests. In this way, it helps to minimise the overall threat score of the datacentre. We keep the benchmark for the standard CVSS score as mention in Table 3. For experiment purpose we have considered low and medium threat analysis score as minimum while the high and critical score as maximum. The cloud service providers can take it to more granular level. We propose the security strategy for reducing the datacentre threat analysis score while placing the new VM request.

Figure 4 Algorithm for VM selection

1. New VM request (TA_{VM}, TA_{NwVM})
2. Calculate the TA_{Host}
3. Calculate the $TA_{permissible}$
4. Calculate the $TA_{Utilization}$
5. Calculate the $TA\ host_{permissible-min}$, $TA\ host_{permissible-max}$, $TA\ host_{permissible-mean}$
6. Calculate the $TA_{Utilization-min,}$ $TA_{Utilization-max,}$ $TA_{Utilization-mean}$
7. Select the pool of TA_{Host} from the datacentre where $TA_{HostSelected} < TA_{permissible}$
8. Compare if TA_{VM}==max && TA_{NwVM}==max

   Select $TA\ host_{permissible-min}$ and $TA_{Utilization-min}$
9. Compare if TA_{VM}==max && TA_{NwVM}==min,

   Select $TA\ host_{permissible-mean}$ and $TA_{Utilization-max}$
10. Compare if TA_{VM}==min && TA_{NwVM}==min,

    Select $TA\ host_{permissible-max}$ and $TA_{Utilization-mean}$
11. Compare if TA_{VM}==min && TA_{NwVM}==max,

    Select $TA\ host_{permissible-mean}$ and $TA_{Utilization-min}$

The algorithm accepts the new VM request and calculates the threat analysis associated with VM, host, host utilisation and the permissible value by the equations mentioned above. Depending on the value of TA_{VM} the placement strategy is decided. Here we are assuming the values of TA_{VM} as max and min where max value lies between [5, 7] and min value lies between [1, 4.9]. Threat score values for the VM above 7 will not be considered suitable for placement. In order to keep the ODTS minimum, the four strategies are drawn. Our approach maps the VM instance with appropriate host in such a way that the risk is distributed among the hosts present in datacentre. While achieving this goal, more active hosts are observed in datacentre which increases the

energy consumption. Security is considered as primary goal along with VM resource utilisation requirements before VM placement.

Table 3 Strategy for reducing the datacentre threat

Strategy	TA_{VM}	TA_{NWVM}	*Host selection*
1	Max	Max	$TA\ host_{(permissible-min)}$, $TA_{(Utilisation-min)}$
2	Max	Min	$TA\ host_{(permissible-mean)}$, $TA_{(Utilisation-max)}$
3	Min	Min	$TA\ host_{(permissible-max)}$, $TA_{(Utilisation-mean)}$
4	Min	Max	$TA\ host_{(permissible-mean)}$, $TA_{(Utilisation-max)}$

4 Simulation and results

We have used cloud simulator tool for simulating the cloud environment. CloudSim is a framework for modelling and simulation of cloud computing infrastructures and services (Calheiros et al., 2011). We have used CloudSim packages like CloudSim2., Org.cloudbus.CloudSim, CloudSim.ext for simulation of the algorithm and cloud analytics is used to show the user interface and plotting the graph. The policy classes from org.cloudbus.CloudSim are used for imitating the policy behaviour of a cloud component. the The classes that comes under this category: VMAllocationPolicy, CloudLetSchedulingPolicy, VMSchedulingPolicy, UtilisationModel. The CloudSim packages CloudSim.ext are modified and jar files are added in order to accept the above stated threat analysis. The CloudSim gui screens are added using Javabeans. The CVSS score is gathered for top 50 vulnerabilities in top 10 operating system, virtual machine manager, ports and used for the simulation purpose. Table 4 shows the details considered.

For the experimental purpose we have considered one datacentre with 800 physical machines of two types and virtual machines from {10 to 1,500} in the below stated interval of two types, with the following configurations shown in Tables 5 and 6.

Table 4 Vulnerabilities considered for VM, PM, VMM, network

Top 10 operating system	*Most popular VMM*	*Commonly used ports*
Debian Linux	Openstack	Core Ftp/21
Windows 10	KVM	SSH/22
Ubuntu Linux	POWER Hypervisor IBM	SMTP/25
Mac OS X	XEN	DNS and WINS Server Could/53
Linux Kernel	Windows Hyper-V	HTTP/80
Windows Server 2016	Vmware Esxi	HTTPS/443
Windows Server 2008	Oracle VirtualBox	TCP
Windows 7		UDP
Windows Server 2012		

CloudSim is a well-known cloud simulator having simple VM allocation policy which follows the default power aware best fit decreasing order VM placement and power model for used PMs. We have compared our approach with this policy to find overall threat analysis. We have considered the check on the permissible risk while placing the

new VM request which results in lower values for the datacentre risk score as compared to simple power aware best fit decreasing policy. Workload traces from dataset PlaneLab 22-03-2011 are selected to conduct experiment.

Table 5 Virtual machine specification

VM specification	*Type 1*	*Type 2*
Total MIPS	2,500	1,000
Total processor units	1	1
Total RAM	1 GB	1 GB
Total bandwidth	100 Mbits/s	100 Mbits/s
Total storage size	2.5 GB	2.5 GB

Table 6 Physical machine specification

PM specification	*Type 1*	*Type 2*
Total MIPS	2,660	1,860
Total processor units	2	2
Total RAM	8 GB	8 GB
Total bandwidth	1 GB	1 GB
Total storage size	80 GB	80 GB

Figure 5 shows that when increasing number of VM's are created in the datacentre from 10 to 1,500 keeping the α (0.5, 0.3, 0.2) there is an increase in overall datacentre threat score. It is observed that in two cases 30, and 40 number of VMs, the threat score exceeds as when compared with the PABFD selection policy, but when the number of VM's increases the ODTS is observed to increase within limits by controlling the outliers. Figure 6 depicts the energy consumption comparison for the same priority values between Secure policy and PABFD. It is observed that the energy consumption increases by average 9% for secure policy. In 70% of the cases for secure policy, the datacentre threat score is lower than the ODTS which indicates lesser attack surface for the coresidency attacks. This ensures to keep the threat level under control and strengthens the trust among customers and cloud service providers.

To find the optimum priority values we repeated the experiments with α (0.6, 0.25, 0.15) as shown in Figure 6 and observed that there is a significant decrease of 11% in the ODTS but Figure 8 shows sharp increase of 13% in the energy consumption when compared with PABFD selection policy. In order to limit the ODTS, the datacentre selects the physical machine with lower host threat score and also limits the resource utilisation hence adding more number of active physical machines to the datacentre. Cloud service providers can offer both level of security as a service as per client requirement. In the related work section current research work has been reviewed. Further we compare our approach with three distinct studies of Agarwal and Duong (2019), Azar et al. (2014) and Yu et al. (2014). With the same simulation environment in CloudSim with 800 physical machines of two types and by adding the number of virtual machines from 10 to 1,500, threat score for overall datacentre was calculated. Host threat score is likewise low if datacentre threat score is low. It is observed from the results shown in Figure 9 that our approach has lower threat score for most of the iterations compared with three studies, except in two cases when less number of virtual machines are spinned. Agarwal and Duong demonstrated better performance

when 30 virtual machines were used, while Azar et al. demonstrated better performance when 50 virtual machines were spinned. When higher number of virtual machines are placed the results are better in each iteration.

Figure 5 Threat score with priority values as (0.5, 0.3, 0.2) (see online version for colours)

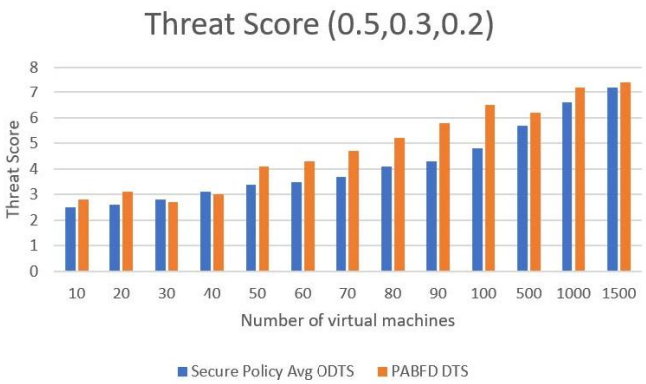


Figure 6 Energy consumption for (0.5, 0.3, 0.2) (see online version for colours)

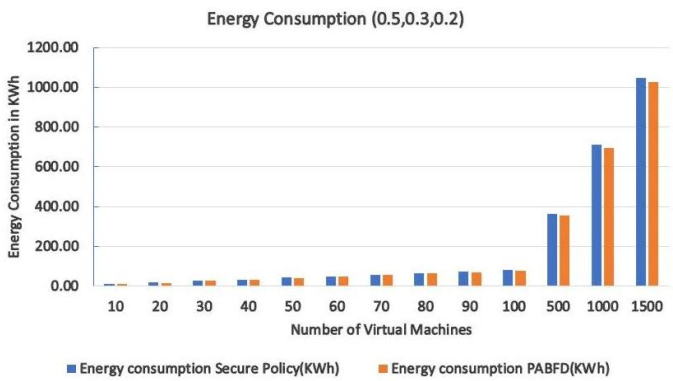


Figure 7 Threat score with priority values as (0.6, 0.25, 0.15) (see online version for colours)

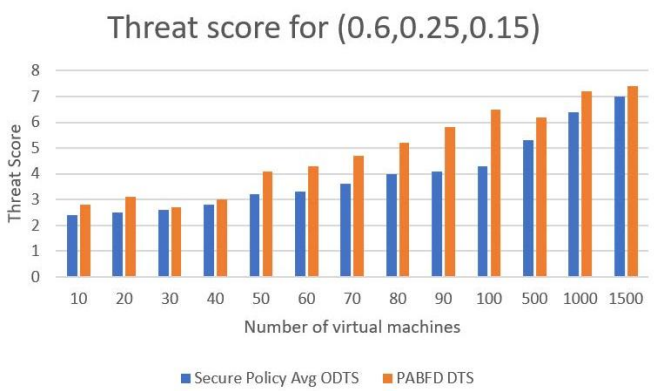


Figure 8 Energy consumption for (0.6, 0.25, 0.15) (see online version for colours)

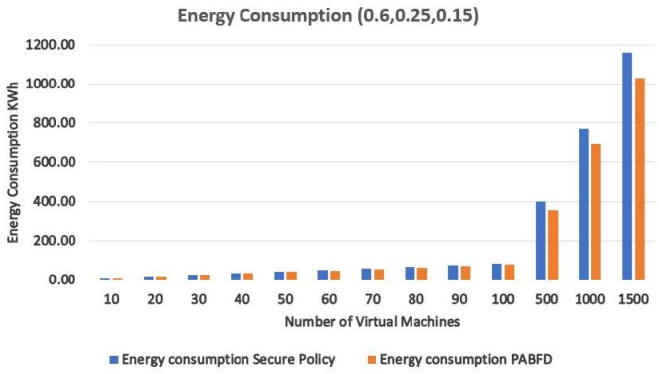


Figure 9 Threat score comparison of proposed secure policy with three other studies (see online version for colours)

Placement of the virtual machine in cloud datacentre after considering security with respect to virtual machine, network, co-located virtual machines and virtual machine manager on the basis of priority of severity impact adds novelty to the work. Our approach also shows financial impact in terms of cost saving towards carbon footprint while offering the secured virtual machine placement policy.

5 Conclusions

In this paper, we provide a priority-based secure virtual machine allocation policy which will do the threat assessment before host selection. We estimate the overall datacentre threat score by using 5-dimensional threat assessment model and follow the secure policy algorithm to select the host which keeps the overall datacentre threat score low in order to avoid co-residency.

With the simulation results we are able to statistically prove that ODTS reduces by average value of 9% and maximum of 18% when compared with

PABFD policy having the maximum increase of 4% in energy consumption when the priority is set to (0.5, 0.3, 0.2) for the network, VMM along with hosted VM's and PM respectively. It is also observed that when the priority is set to (0.6, 0.25, 0.15) for the network, VMM along with hosted VM's and PM respectively, the ODTS can be further reduced to average value of 13% and maximum of 24% but there is increase of average energy consumption by 8% when compared with power aware best fit decreasing (PABFD) policy.

Future scope may include calculating and comparing the improvement in SLA at datacentre level or host level with the past studies and to consider the threat score of already placed VMs which are subject to continuous changes as a part of software development life cycle. This process can also result in migration of already placed VM's to manage the ODTS as per SLA.

References

Afoulki, Z., Bousquet, A. and Rouzaud-Cornabas, J. (2011) *A Security-Aware Scheduler for Virtual Machines on IaaS Clouds*, Report, Universite D'Orleans, pp.1–13 [online] https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a7b8f5feb44ed05c9399443c8d466c7ee404526b.

Agarwal, A. and Duong, T.N.B. (2019) 'Secure virtual machine placement in cloud data centers', *Future Generation Computer Systems*, Vol. 100, pp.210–222.

Al-Haj, S., Al-Shaer, E. and Ramasamy, H.V. (2013) 'Security-aware resource allocation in clouds', *2013 IEEE International Conference on Services Computing*, pp.400–407.

Azar, Y., Kamara, S., Menache, I., Raykova, M. and Shepard, B. (2014) 'Co-locationresistant clouds', *Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security*, pp.9–20.

Bogdanoski, M., Suminoski, T. and Risteski, A. (2013) 'Analysis of the SYN food DoS attack', *International Journal of Computer Network and Information Security (IJCNIS)*, Vol. 5, No. 8, pp.1–11.

Calheiros, R.N., Ranjan, R., Beloglazov, A., Rose, C.A.D. and Buyya, R. (2011) 'CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms', *Software: Practice and Experience (SPE)*, Vol. 10.

Escheikh, M., Tayachi, Z. and Barkaoui, K. (2018) 'Performability evaluation of server virtualized systemsunderbursty workload', *IFAC-PapersOnLine*, Vol. 51, No. 7, pp.45–50.

Feizollahibarough, S. and Ashtiani, M. (2021) 'A security-aware virtual machine placement in the cloud using hesitant fuzzy decision-making processes', *The Journal of Supercomputing*, Vol. 77, pp.5606–5636.

Fernandez, E.B., Monge, R. and Hashizume, K. (2013) 'Two patterns for cloud computing: secure virtual machine imagerepository and cloud policy management point', *Proceedings of the 20th Conference on Pattern Languages of Programs*, p.15.

Gaggero, M. and Caviglione, L. (2018) 'Model predictive control for energy-effcient, quality-aware, and secure virtual machine placement', *IEEE Transactions on Automation Science and Engineering*, Vol. 16, No. 1, pp.420–432.

Goasduff, L. and Stamford, C. (2021) *Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences*, Gartner [online] https://www.gartner.com/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences.

Grobauer, B., Walloschek, T. and Stocker, E. (2010) 'Understanding cloud computing vulnerabilities', *IEEE Security & Privacy*, Vol. 9, No. 2, pp.50–57.

Gruschka, N. and Jensen, M. (2010) 'Attack surfaces: a taxonomy for attacks on cloud services', *2010 IEEE 3rd International Conference on Cloud Computing*, pp.276–279.

Han, J., Zang, W., Liu, L., Chen, S. and Yu, M. (2018) 'Risk-aware multi-objective optimized virtual machine placement in the cloud', *Journal of Computer Security*, Vol. 26, No. 5, pp.707–730.

Han, Y., Chan, J., Alpcan, T. and Leckie, C. (2015) 'Using virtual machine allocation policies to defend against co-resident attacks in cloud computing', *IEEE Transactions on Dependable and Secure Computing*, Vol. 14, No. 1, pp.95–108.

Hasan, M.M. and Rahman, M.A. (2020) 'A signaling game approach to mitigate co-resident attacks in an IaaS cloud environment', *Journal of Information Security and Applications*, Vol. 50, p.102397.

Lin, W. and Lee, D. (2012) 'Traceback attacks in cloud–pebbletrace botnet', *2012 32nd International Conference on Distributed Computing Systems Workshops*, pp.417–426.

Liu, F., Ren, L. and Bai, H. (2014) 'Mitigating cross-VM side channel attack on multiple tenants cloud platform', *J. Comput.*, Vol. 9, No. 4, pp.1005–1013.

Liu, S.T. and Chen, Y.M. (2011) 'Retrospective detection of malware attacks by cloud computing', *International Journal of Information Technology*, Vol. 1, No. 3, pp.280–296.

Maris, A. and Wiles, D. (2019) *Common Vulnerability Scoring System* [online] https://www.first.org/cvss/v3-1/cvss-v31-specificationr1.pdf.

Mell, P., Scarfone, K. and Romanosky, S. (2007) 'A complete guide to the common vulnerability scoring system version 2.0', in *FIRST – Forum of Incident Response and Security Teams*, Vol. 1, p.23.

OWASP (2022) *Web Application Firewall*, OWASP.

Parast, C., Sindhav, S. and Nikam, S. (2022) 'Cloud computing security: a survey of service-based models', *Computers & Security*, Vol. 114, p.102580.

RA, V.C. (2016) *The Treacherous 12* [online] https://downloads.cloudsecurityalliance.org.

Ristenpart, T., Tromer, E., Shacham, H. and Savage, S. (2009) 'Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds', *Proceedings of the 16th ACM Conference on Computer and Communications Security*, pp.199–212.

Szefer, J. and Lee, R.B. (2012) 'Architectural support for hypervisor-secure virtualization', *ACM SIGPLAN Notices*, Vol. 47, No. 4, pp.437–450.

Vaquero, L.M., Rodero-Merino, L. and Morán, D. (2011) 'Locking the sky: a survey on IaaS cloud security', *Computing*, 24 November, January, Vol. 91, pp.93–118 [online] https://doi.org/10.1007/s00607-010-0140-x 2010.

Yu, S., Gui, X., Lin, J., Tian, F., Zhao, J. and Dai, M. (2014) 'A security-awareness virtual machine management scheme based on Chinese wall policy in cloud computing', *The Scientifc World Journal*, Vol. 2014, Article ID 805923, 12pp [online] https://doi.org/10.1155/2014/805923.

Zhang, Y., Juels, A., Oprea, A. and Reiter, M.K. (2011) 'Homealone: co-residency detection in the cloud via side-channel analysis', *2011 IEEE Symposium on Security and Privacy*, pp.313–328.

Zhou, F., Goel, M., Desnoyers, P. and Sundaram, R. (2013) 'Scheduler vulnerabilities and coordinated attacks in cloud computing', *Journal of Computer Security*, Vol. 21, No. 4, pp.533–559.