International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7414
***Article Received**: 06 May 2023 **Revised:** 28 June 2023 **Accepted:** 27 July 2023*

Security Aware Virtual Machine Allocation Policy to Improve QoS

Aparna Prashant Bhonde[1], Dr. Satish Devane[2]
[1]Department of Infromation Technology
Datta Meghe College of Engineering , Airoli
Mumbai, India
aparna.bhonde@dmce.ac.in
[2]Department of Infromation Technology
Datta Meghe College of Engineering , Airoli
Mumbai, India
satish@dmce.ac.in

Abstract— Cloud service providers find managing the energy consumption for datacentres as a critical operation. Significant energy is being used by a rising spike in the number of data centres. To overcome this challenge datacentres, attempt to reduce the number of active physical servers by carrying out virtual machine consolidation process. However, due to inadequate security measures to verify hostile cloud users, the security threats on cloud multitenancy platform have escalated. In this paper we propose energy efficient virtual machine consolidation using priority-based security aware virtual machine allocation policy to improve datacentre security. The proposed security solution considers the host threat score before virtual machine placement, which has reduced the security threats for co-residency attacks without impacting datacentre energy consumption.

Keywords- Virtual machine security, virtual machine allocation policy, virtual machine consolidation, Virtual machine attacks, co-residency attacks

I. INTRODUCTION

Cloud computing is predominantly known for heterogeneous architecture with variation in hardware and is abstracted from end users. It also provisions on-demand self-service, extensive network connectivity, a variety of client devices, resource pooling, quick elasticity, and quantifiable costs with a pay-per-use pricing structure. Earlier cloud used to have standard group of common hardware but with the advent of distributed and resource sharing environment there is development in its architecture. To fulfil demands by cloud users for high availability, scalability with the required performance is the goal for cloud service providers. It is possible to achieve stated goals with less cost and energy due to advancements in virtualization technology within the datacentres across all resources.

According to a recent survey, over the past three years, businesses have paid an increasingly large price for data centre downtime [1]. Among the various reasons for cloud services downtime is cloud attacks related to distributed de- nial of service (DDOS). Cloud service providers have ser- vice level agreement violations (SLAV), which hinders them from retaining customers’ trust [2]. Service providers have adopted innovative ways to keep check on energy required for computation by consolidation of Virtual Machines (VM) on lesser number of physical severs. This technique has surely helped in reducing the cost of datacentre but moving VMs all over a Physical Machine (PM) poses apparent security problems because it is vulnerable to cyberattacks in absence of monitored security policy. Although datacentres follow virtual private network isolation, there is a possibility of security threat due to malicious VM gaining access on PM [3] . Cloud computing being an integrated system inherits many traditional threats from network, system or components. Some threats arising due to multitenancy, virtualization are specific and are bound to cloud environment resulting in DDOS, cache based side channels or Cross Site Scripting (CSS) and reducing the performance by 95% and increasing the overheads [4] .

Selection of server after considering threats in order to host new virtual machine instance is the novel idea which is proposed to mitigate VM based attacks due to co-residency during VM consolidation process to reduce the SLAV due to attacks on datacentre. Threats at different levels of datacentre like physical machine, virtual machine, virtual machine manager and network communication are prioritised and calculated based on metrics. Initial host machine is selected on the basis of threat score and resource requirements, to avoid co- residency such that overall threat score remains less than the mean of host threat score for datacentre. A series of simulation results show that using proposed solution, the virtual machine attacks can be mitigated for co-residency attacks controlling the SLA violations and energy consumption. The proposed idea gives an additional security in VM placement with minimal impact on energy and improves quality of service.

The rest of the paper is organised as follows. In section 2, the background and motivation for this research is dis- cussed. In section 3, priority-based security aware Virtual machine consolidation algorithm is presented. Later in section 4, experimental setup for simulation is discussed followed by simulation results and its analysis in section 5. Section 6 comprises of conclusion and future scope in this area.

II. BACKGROUND AND MOTIVATION

Cloud datacentres aim to reduce energy cost. In order to reduce power usage, VM consolidation is proposed as a method of green cloud computing. There are multiple objectives for VM consolidation, includes optimising resource, traffic, cost, performance and energy. Security for the virtual machines is generally overlooked in view of VM consolidation which may lead to obtain co-residency by adversary. Gaining co-residency involves basic step that introduces threats such as fate sharing and cache-based side channel attacks controlled by attacker [5].All co-located virtual machine instances hosted on same physical machine evidently shares physical resources. In such a case, a malicious attacker in control of a VM may attempt to seize control of the resources of other VMs or establish covert channel, resulting in a denial-of-service assault on other clients. Another possibility is to exploit virtual machine manager logical units and sniff other client data. Attacker searches for the target by observing cache usage, traffic rates and load on specific network address [6]. Information leakage through side channels happens when the adversary and the target machines reside on the same physical server.

Assaults on web services account for up to 60% of attacks targeting organisations. According to owasp top 10 vulnerabilities, injections and sensitive data exposure are commonly used for exploiting data [7]. By using advanced scripting techniques even public cloud providers Amazon and eucalyptus cloud can be compromised [8]. CSP facilitates wide range of options and services which are equally available to all the cloud users. The challenge faced by CSP is to distinguish between genuine user and the rogue machine which can use all the cloud features to mount a distributed denial of service attack [9]. Users may be required to pay significant sums as a result of DDOS assaults in utility-based payment system. Attacker can compromise network interface driver present in virtual machine manager for DDOS attack which may result even in crashing OS kernel damaging virtual machines hosted on it [10] . All the above threats encourage to discover techniques to secure virtual machines that share resources in multitenant cloud environment. Cloud allocation policy takes an important role where the virtual machine instances are mapped with physical machines in datacentre. Many a times security for the virtual machines is not considered in view of VM consolidation. We consider security aspect, energy consumption as well as SLA violations while hosting or migrating virtual machines which improves security during VM consolidation process. This assures the cloud service providers to maintain overall SLA violations and build trust with clients and mitigate virtual machine attacks

III. SECURITY AWARE VIRTUAL MACHINE CONSOLIDATION USING ATTACK PRIORITY

The process of consolidating virtual machines (VMs) involves methods for selecting the most effective algorithm for VM migration and placement on the suitable host. Virtualization and consolidation are being used more frequently in data centres to accommodate numerous concurrently running applications. Live migration can be used for load balancing and to perform infrastructure maintenance without significantly affecting the availability and responsiveness of the application resulting in effective management of the physical resources. Cloud adopts virtualization techniques and shares the resources to use cloud infrastructure in an efficient and optimal way. While achieving the goal of VM consolidation there is a possibility of security breach due to co-location of malicious vm on the same physical machine [3]. In order to overcome this issue there is a need to consider security while consolidating the VM in the datacentre. We propose the priority-based security aware VM consolidation, which calculates the overall datacentre threat score (ODTS) and considers the physical machines with minimum permissible value for threat score and energy utilization while consolidation.

A. Proposed methodology

We propose a priority-based virtual machine placement policy which selects the host from datacentre after calculating priority-based threat score for each host in datacentre. To achieve this goal, we follow the threat assessment model which considers threat associated from all stages within the datacentre. Following Figure 1 shows threat assessment model.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
DOI: https://doi.org/10.17762/ijritcc.v11i9s.7414
***Article Received**: 06 May 2023 **Revised:** 28 June 2023 **Accepted:** 27 July 2023*

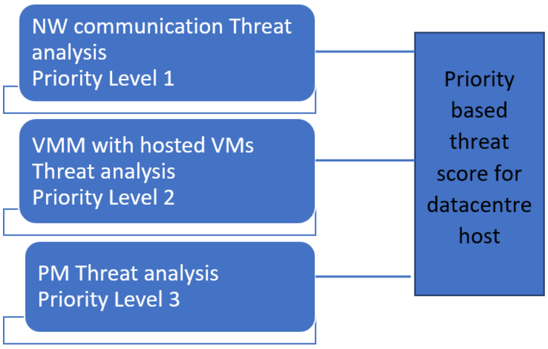
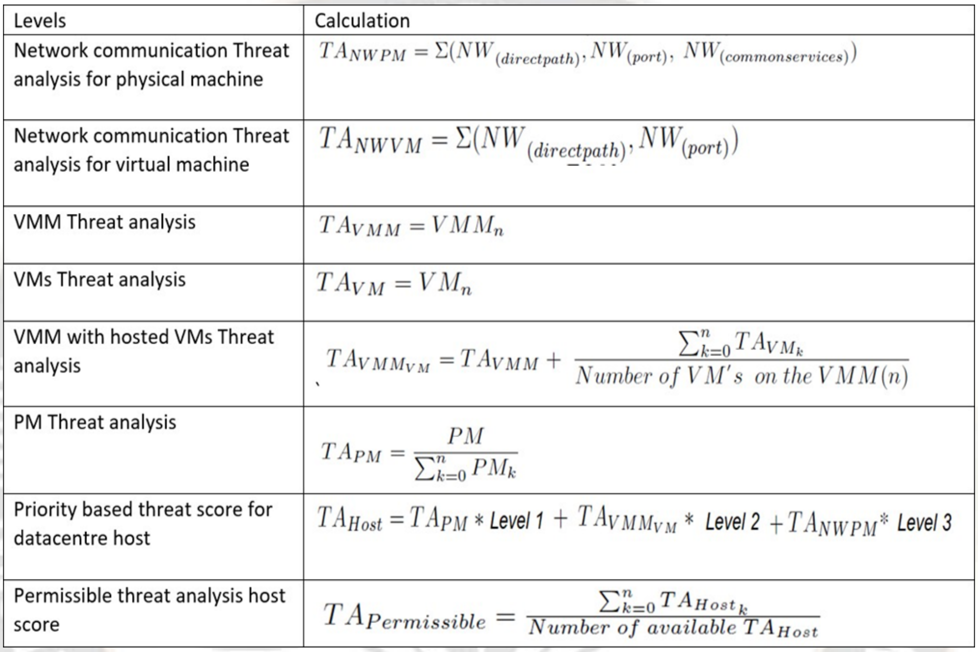

NW communication Threat analysis
Priority Level 1
VMM with hosted VMs Threat analysis
Priority Level 2
PM Threat analysis
Priority Level 3
Priority based threat score for datacentre host

Figure. 1. Architecture for priority selection

Threat assessment model calculates physical machine threats, threats associated with virtual machine manager along with the Virtual machines hosted on it and threats due to established network communication. Among the threats men- tioned, severity of network threat is at level 1 as it is observed as biggest security challenge to keep check on network attacks [11] . The network paths considered are common services shared, direct paths and ports which are used for establishing communication with other vms within datacentre. Threats associated with virtual machine manager along with the virtual machines hosted on it is at level 2, where vulnerability score of virtual machine manager and consolidated threat score for all vm instances are taken. Physical machine threat analysis is a static analysis and is calculated on the basis of vulnerabilities associated with physical machines. We prioritise the threat as level 3 and use normalisation function for the many physical machines present in the datacentre. Each level is assigned a weight for host threat analysis score where the priority is set as level1>level2>level3, where, level 1 is the weight given for the network threat, level 2 is the weight given for the VMM along with the hosted VM's on it and level3 is for physical machine threat.



Levels	Calculation
Network communication Threat analysis for physical machine	$TA_{NWPM} = \Sigma(NW_{(directpath)}, NW_{(port)}, NW_{(commonservices)})$
Network communication Threat analysis for virtual machine	$TA_{NWVM} = \Sigma(NW_{(directpath)}, NW_{(port)})$
VMM Threat analysis	$TA_{VMM} = VMM_n$
VMs Threat analysis	$TA_{VM} = VM_n$
VMM with hosted VMs Threat analysis	$TA_{VMM_{VM}} = TA_{VMM} + \frac{\sum_{k=0}^{n} TA_{VM_k}}{Number\ of\ VM's\ \ on\ the\ VMM(n)}$
PM Threat analysis	$TA_{PM} = \frac{PM}{\sum_{k=0}^{n} PM_k}$
Priority based threat score for datacentre host	$TA_{Host} = TA_{PM} * \textit{Level 1} + TA_{VMM_{VM}} * \textit{Level 2} + TA_{NWPM} * \textit{Level 3}$
Permissible threat analysis host score	$TA_{Permissible} = \frac{\sum_{k=0}^{n} TA_{Host_k}}{Number\ of\ available\ TA_{Host}}$

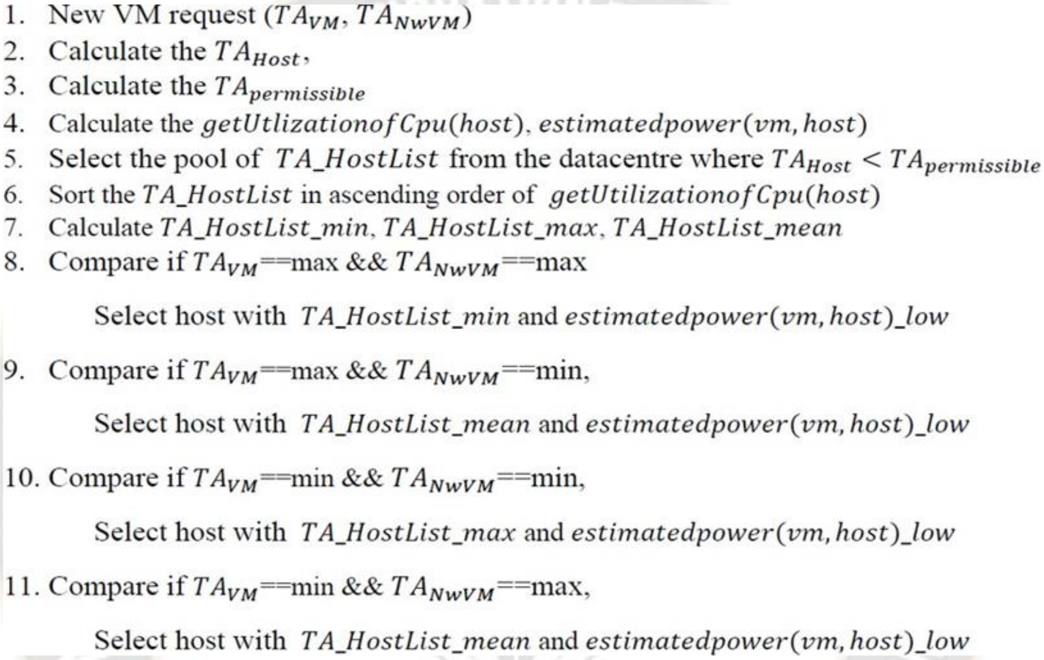
Fig. 2. Calculation of priority-based threat score

B. Calculating the priority-based threatscore

1. Network threat analysis for PM: If the co-residency of the attackers VM is successfully achieved, it can potentially exploit other VMs on the host. An analysis of network threats can be conducted through direct communication paths to the virtual machines, port communication, and communication through common services. Due to the increase in attack complexity with the number of hops, this study is limited to direct paths. To calculate the host threat score in the datacenter, the network threat associated with the virtual machines already hosted on a particular physical machine is considered.
2. Network threat analysis for VM: The determination of network vulnerability assessment for the recently requested virtual machine can be ascertained through the identification of direct pathways. As the virtual machine will be incorporated into a virtual private cloud, the accessible communication ports will be discernible.
3. Threat analysis for VM and VMM: The evaluation of the threat assessment score for the virtual machine monitor is performed by taking into account the self-vulnerability and the virtual machines hosted on said monitor. This analysis involves assessing the vulnerabilities associated with various virtual machine

monitors, such as Xen and KVM, within the datacenter. The analysis of virtual machine threats involves evaluating the vulnerabilities linked to the selected image for different virtual machines.

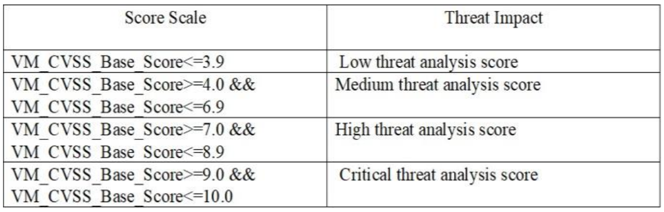
4. Physical machine threat analysis: This is a form of threat analysis that adopts a static approach, whereby the vulnerabilities that are linked to the physical machines located within the datacentres are considered.
5. Permissible threat analysis host score: The proposed innovative methodology computes the score for threat assessment of every host in the datacentres, including the virtual machine's threat score. To ensure the security of the datacentre, the allowable threat score for the entire datacentre must be lower than the average threat analysis host score. Moreover, the physical machine's threat score should be below the permissible threat analysis score when it is selected to accommodate new VM requests. This approach effectively reduces the overall threat score of the datacentre, hence, enhancing its security.



```
1.  New VM request ($TA_{VM}$, $TA_{NwVM}$)
2.  Calculate the $TA_{Host}$,
3.  Calculate the $TA_{permissible}$
4.  Calculate the $getUtlizationofCpu(host)$, $estimatedpower(vm, host)$
5.  Select the pool of $TA\_HostList$ from the datacentre where $TA_{Host} < TA_{permissible}$
6.  Sort the $TA\_HostList$ in ascending order of $getUtilizationofCpu(host)$
7.  Calculate $TA\_HostList\_min$, $TA\_HostList\_max$, $TA\_HostList\_mean$
8.  Compare if $TA_{VM}$==max && $TA_{NwVM}$==max
        Select host with $TA\_HostList\_min$ and $estimatedpower(vm, host)\_low$
9.  Compare if $TA_{VM}$==max && $TA_{NwVM}$==min,
        Select host with $TA\_HostList\_mean$ and $estimatedpower(vm, host)\_low$
10. Compare if $TA_{VM}$==min && $TA_{NwVM}$==min,
        Select host with $TA\_HostList\_max$ and $estimatedpower(vm, host)\_low$
11. Compare if $TA_{VM}$==min && $TA_{NwVM}$==max,
        Select host with $TA\_HostList\_mean$ and $estimatedpower(vm, host)\_low$
```

Fig. 4. Security aware virtual machine consolidation algorithm

The Figure 2 shows all the stages at which datacentre threat score is calculated as mentioned. The CVSS is a popular tool for evaluating the vulnerabilities of software or hardware (Common Vulnerability Scoring System). Vulnerability scanner tools like Nessus and Qualys are used to create the vulnerability list for each PM or VM. On a scale of 0 to 10, the CVSS score assigns vulnerabilities a severity rating. We can choose CVSS as our reference point to standardise all vulnerability scores if alternative tools are used to rate vulnerabilities as shown in Figure 3.



Score Scale	Threat Impact
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

Fig. 3. Figure standard CVSS score

The new approach that has been proposed, determines both the threat score for the virtual machine and the threat assessment score for each host that is present in the datacenters. The permitted threat analysis host score, which is determined by the mean of TA Host, should be lower than the permissible treat score for the entire datacenter. When a physical machine is selected to host a new VM request, the selected host threat score must maintain lower permissible threat analysis host score. This contributes to keep overall datacenter's total threat score under limit. Low and medium threat analysis scores have been classified as minimum, whereas high and critical scores have been classified as maximum for experimentation. Cloud service providers can add more detailed levels. We propose a security approach to minimize the datacenter threat analysis score when a new VM request is received.

The proposed algorithm Figure 4 calculates vm threat score and network vulnerability threat score for new VM request. Vulnerability for each host in the datacentre is calculated and compared with permissible value for datacentre threat score. getUtilizationofCpu() function gives the current utilization of cpu in percentage and estimatedpower function checks overall power consumption by server after expected future migration. Each host is compared with the permissible threat analysis score and a host list is formed. Based on CPU usage, the selected hosts are listed in ascending order. Depending upon the VM threat score of the new VM request, finally appropriate host is selected according to the conditions mention in the algorithm. The stated proposed solution is implemented in cloudSim and results were observed.

IV. SIMULATION SETUP

In order to simulate and test stated approach, CloudSim framework is available to simulate infrastructures and application services [12]. It is an opensource tool where researchers can modify programmatically using java classes and extend it for their approach. CloudSim has the ability to define datacentres, compute power, VMs, hosts and various scheduling and allocation policies using these classes. We have done effective modifications to calculate threat score for the datacentre at each level mentioned in sec 3. above.

Workload traces from CoMon project, dataset PlanetLab (03032011) are selected to conduct experiment. The range of the samples average workload was between 5% and 30%.These workloads provide 288 data collection points for CPU usage at 5 min interval for a specific VM at any given time. Power consumption with respect to power usage by host with host utilization table was designed for comparison. The ideal relation between the CPU utilization and power consumption is shown in Figure 5. Datacentre simulation comprised of 800 heterogeneous physical machines of 2 types and 1052 VMs. Their specifications are as stated HP ProLiant ML110 G4 (Intel Xeon 3040, 2 cores 1860 MHz, 4 GB), and HP ProLiant ML110 G5 (Intel Xeon 3075, (2 cores 2660 MHz, 4 GB). Power consumption patterns are referred from real data provided by SPECpower definition [13]. Figure 5 shows the Server power consumption based on load and it is seen 30% increase in power consumption while the load changes from 0% to 100%.

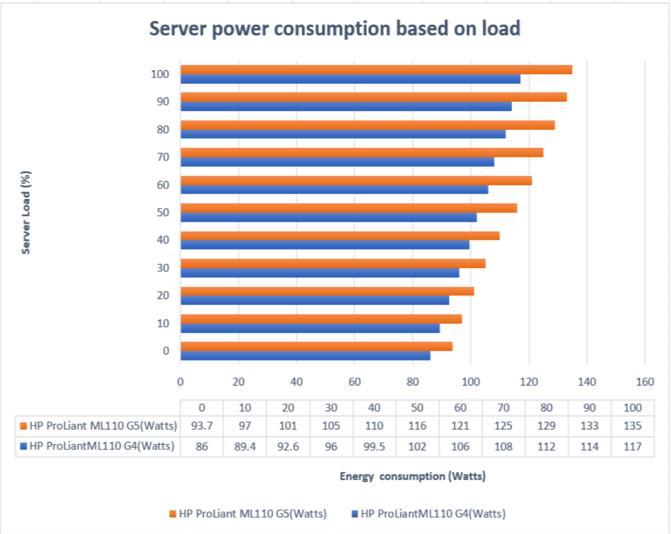


Fig. 5. Server power consumption based on load

The virtual machine specifications are as shown in Table I. Migration cycle is set after every 60 minutes upon which our novel approach will check for utilization and power consumption for every host. The check will also get triggered when a new VM request is received by the cloud service provider, whichever is earlier

TABLE I
VIRTUAL MACHINE SPECIFICATION

VM Specification	Type 1	Type 2	Type 3	Type 4
Total MIPS	2500	2000	1000	500
Total processor units	1	1	1	1
Total RAM	870	1740	1740	613
Total bandwidth	100 Mbits/s	100 Mbits/s	101 Mbits/s	102 Mbits/s

In the experimentations, VMs and the hosts were tested for observing performance low to medium load. The hosts and Vms were increased in the interval of 100 and 200 respectively. We set the limit of hosting 8 VMs per PM for experiment.Host overload detection algorithm and VM selection algorithms available in cloudsim were modified with priority based security aware vmap to compare the power usage and SLA violations.

V. RESULTS AND DISCUSSIONS

For each host in the datacentre, threat score is calculated as discussed in sec 3. To understand the change in energy consumption, we took low to medium workload and incremented host threat score level from 2 to 10. The simulation result is shown in Figure 6 where Y axis represents energy in kWh and X axis represents the host threat score in the cloud datacentre. It is observed that when the host threat score is increased from

DOI: https://doi.org/10.17762/ijritcc.v11i9s.7414
***Article Received**: 06 May 2023 **Revised:** 28 June 2023 **Accepted:** 27 July 2023*

2 to 10, energy consumption increased by 2.08 %. However, it is also observed that when host threat score is selected between 6 to 8, the curve remains stable indicating same no change in number of physical machines to host the VM tasks.

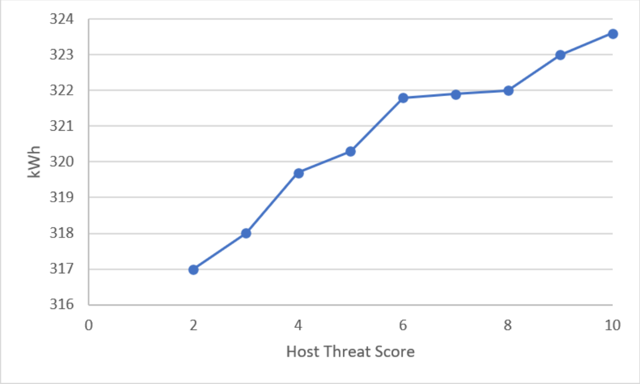


Fig. 6. Security aware VM consolidation comparison for low-medium workload for 800 hosts

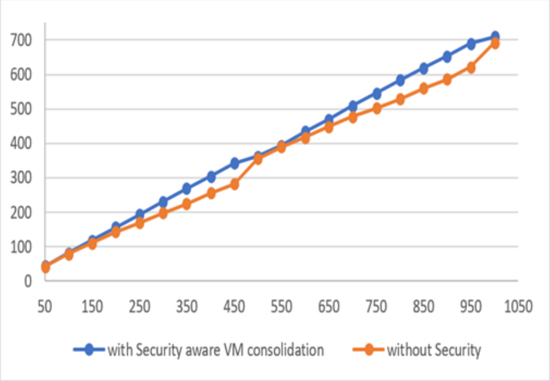


Fig. 7. Energy consumption observed for increasing Virtual machine instances in datacentre

To test the scalability in terms of incrementing VM instances in the datacentre, we simulated as shown in Figure 7 the 800 hosts with host threat score from 3 to 7 and executed virtual machine requests. The virtual machine requests were created in datacentre from 50 to 1000 in 2 situations. One scenario with applying Energy efficient security aware VM consolidation and another without any security. It is observed that energy consumption increases almost linearly when VM instances are created from 50 to 1000 in the datacentre. The simulation was carried out with security aware VM consolidation and compared to without security and noted that average power consumption is increased by 9.4 %. The experiment concludes consistent behaviour for energy consumption for various levels of VM requests in the data centre and our solution is scalable and works with higher number of VM requests without any bottleneck.

TABLE II
SECURE VM ALLOCATION ALGORITHM ENERGY CONSUMPTION, SLAV, ESV

with Priority base security aware policy	Energy consumption (kWh)	Overall SLA violation (%)	(Energy times SLA violations) ESV
Secure-LR-MMT	294	9.06	2663.64
Secure-LRR-MMT	295	9.72	2867.4
Secure-THR-MMT	297	10.04	2981.88
Secure-LRR-MU	301	10.08	3034.08
Secure-IQR-MU	309	10.02	3096.18
Secure-MAD-MMT	310	10.09	3127.9
Secure-MAD-MC	316	10.05	3175.8
Secure-IQR-MMT	312	10.35	3229.2
Secure-LR-MC	326	10.06	3279.56

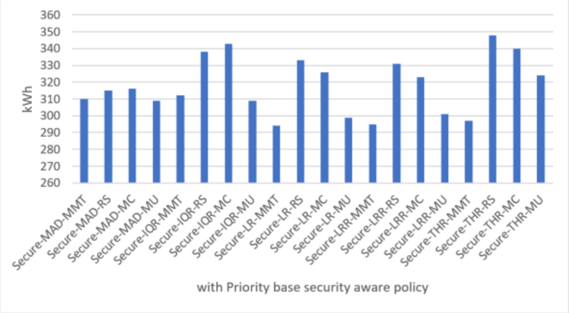


Fig. 8. Energy consumption for Priority based security aware VM consolidation policy

To implement Energy efficient security aware VM consolidation, a variety of VM selection and placement algorithms can be combined into a single VM consolidation pair. VM selection and placement was carried out after application of priority base security aware policy to each pair. First the host threat score was calculated for each host in the datacentre and a pool of hosts which have threat score less than the permissible value were passed to VM consolidation. The results depict that for the policies which works on minimum migration time shows better results compared to maximum correlation and random selection which infers that traditional VM allocation policy gives less weightage to correlation between virtual machines mapped to the host. With the security perspective, mapping virtual machines to hosts is a vital step and priority- based security aware VM consolidation policy considers security while placing the virtual machine instances.

The statics in Table II shows that SLA violations for the secure algorithms state that with prediction of overloaded hosts in LR and LRR Secure Algorithms, the possibility of SLA violations and virtual machine migration to other hosts decreases.

VI. CONCLUSIONS

In this paper we have discussed about priority-based security aware VMAP, to include while virtual machine consolidation process. The proposed algorithm is implemented in CloudSim and analysed cloud behaviour in supervised and regulated environment. Different simulation setups and the resulting findings demonstrate that for ODTS between 6 to 8 there are no significant increases in energy usage when achieving security aware VM consolidation, however shows increase of 2.08% for threat score when increased from 2 to 10. We have arrived to this finding after examining several workloads and computational resources. The proposed solution that uses dynamic VM consolidation has been tested for its scalability and it is observed that it shows similar properties to a non- security-aware VM consolidation. Secure Local Regression Minimum Migration Time version shows 10.88% less energy consumption and 23.12 % lesser energy times SLA violations when compared to secured VM consolidation algorithms. With regard to workload in a data centre, the proposed solution is consistent at both low and high levels of tasks. The scope of this work might be expanded and enhanced to address trust on VM, security, and energy usage.

REFERENCES

[1] J. Shepard, "E N Power," 2016. [Online]. Available: https://eepower.co m/news/unplanned-data-center-outages-cost-nearly-9000-per-minute/

[2] A. Bhonde and S. Devane, "Impact of Cloud Attacks on Service Level Agreement," 2021 International Conference on Communication information and Computing Technology (ICCICT), pp. 1–6, 2021.

[3] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "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, 2009.

[4] T. Zhang, Y. Zhang, and B. Ruby, 2016. [Online]. Available: https://arxiv.org/abs/1603.03404

[5] J. Betz, D. Westhoff, and G. Müller, "Survey on covert channels in virtual machines and cloud computing," Transactions on Emerging Telecommunications Technologies, vol. 28, no. 6, pp. 3134–3134, 2017.

[6] Mr. Kaustubh Patil, Promod Kakade. (2014). Self-Sustained Debacle Repression Using Zig-Bee Communication. International Journal of New Practices in Management and Engineering, 3(04), 05 - 10. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/32

[7] A. Jasti, P. Shah, R. Nagaraj, and R. Pendse, "Security in multi-tenancy cloud," 44th Annual 2010 IEEE International Carnahan Conference on Security Technology, pp. 35–41, 2010.

[8] "OWASP Top 10 Risks," Open Web Application Security Project, 2021.

[9] Yadav, S. S. ., Maan, M. K. ., Kumar, M. S. ., J., K. ., Pund, S. S. ., & Rathod, M. . (2023). A Secure IoT Smart Network Model for the Contributory Broadcast Encryption for the Text Policy Management Scheme. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 42–48. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2530

[10] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "All your clouds are belong to us: security analysis of cloud management interfaces," in Proceedings of the 3rd ACM workshop on Cloud computing security workshop (CCSW '11). Association for Computing Machinery, 2011, pp. 3–14.

[11] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer Communications, vol. 107, pp. 30–48, 2017.

[12] A. Kurmus, M. Gupta, R. Pletka, C. Cachin, and R. Haas, "A comparison of secure multi-tenancy architectures for filesystem storage clouds," in ACM/IFIP/USENIX International Conference on Distributed Systems Platforms and Open Distributed Processing. Springer, 2011, pp. 471– 490.

[13] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, "DDoS attacks in cloud computing: Issues, taxonomy, and future directions," Computer Communications, vol. 107, pp. 30–48, 2017.

[14] R. Buyya, R. Ranjan, and R. N. Calheiros, “Modeling and simulation of scalable Cloud computing environments and the CloudSim toolkit: Challenges and opportunities,” 2009 international conference on high performance computing & simulation, pp. 1–11, 2009.

[15] Jóhann, Þorvaldsson, Koskinen, P., Meer, P. van der, Steiner, M., & Keller, T. Improving Graduation Rates in Engineering Programs Using Machine Learning. Kuwait Journal of Machine Learning, 1(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/110

[16] B. info, “SPEC’s Benchmarks and Tools,” 2011. [Online]. Available: https://www.spec.org/benchmarks.html\#power