Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 3, pp. 719–727
DOI : 10.47974/JDMSC-1744

Multi criteria optimize secure VM placement strategy against cross VM attack

Hansraj [†]
Pradeep Kumar Tiwari [*]
Department of Information Technology
Manipal University Jaipur
Jaipur
Rajasthan
India

Alka Chaudhary [§]
Department of Information Technology
Amity Institute of Information Technology
Noida
Uttar Pradesh
India

Abstract

Cloud computing is becoming more and more popular, but it also presents several security challenges. VMs are generally rented out on demand to users on large scale. Cloud service providers have numerous issues as a result of the increasing user demand for low-cost and high-performance cloud computing, both in terms of security and resource. One of these difficulties is the "co-residence Cross VM attack," in which attackers use the shared cloud's resource pooling to launch various attacks against their co-residents on shared physical machine (PM). Co-resident attacks, in which malicious users create side channels and steal sensitive data from VMs, are often used by attackers. The goal is to assure secure VM placement while optimizing physical resource in cloud data centers. In this study, we concentrate on safe virtual machine placement techniques that provide security against the co-location-based Cross VM attacks. To find the optimum allocation technique, we further apply the Particle swarm optimization (PSO algorithm motivated by particle swarm and

[†] *E-mail:* **hansrajy@gmail.com**
[*] *E-mail:* **pradeeptiwari.mca@gmail.com (Corresponding Author)**
[§] *E-mail:* **alka.chaudhary0207@gmail.com**

their behavior. The proposed approach may help to make the cloud energy-efficient and secure, according to the findings of the experiments.

Subject Classification: *68-XX, 60K30, 91G20, 03D78.*

Keywords: *Cloud security, Co-resident attacks, Cross VM attack.*

1. Introduction

Cloud Computing Cloud computing became fastest growing segments for both commercial and non-commercial computation applications which has enormous potentials for secure on-demand services with low cost. Users and businesses may profit from cloud computing in a number of ways, including reduced capital costs and operating costs. Cloud computing dynamically allows numerous users access to a shared physical machine. The computational level continues to view the various level of security concerns imposed by the cloud provider as a problem. A virtualization security strategy is used to secure against unwanted access to shared resources, data, and virtual machines (VMs) [1]. In a cloud environment, the cloud provider control the assignment of VMs to PMs through the use of a placement strategy. Secure VM allocation against Co-residency Cross attack, one of the biggest issues with cloud. Cross Virtual Machine (VM) attacks take place as a result of shared resources by service provider between services or clients that use virtualization. [2] In this article, defense against Cross VM Attack, resource allocation, load balancing and energy consumption optimization technique is suggested. A Cloud System Model, which permits mapping between VMs and PMs as well as between VM activities, was used to design this approach. This algorithm's technique also encourages security against Cross VM attack. We evaluated and analyzed the security risk of VM using the CloudSim Simulator and result compared to other secure VM placement techniques that are already in use.

2. Related Work

In this Section, We start by explain the existing co-resident attack and Next, Analysis of past Defending method against Co-residency attack. Recent research has concentrated on reducing security risk and data centers operating costs as a result.

2.1 *Co-residency Cross VM attack and Countermeasures*

Cache-based Cross virtual machine (VM) side channel attacks are difficult to detect because they bypass software isolation protections. Timing is used in cache-based (Cross VM) side channel attacks. In co-resident attacks, malicious users utilize side-channels to gain sensitive data from VMs.

Security of Cloud is service that protects client data and resources against unwanted access. The proposed study analyses security at hypervisors and resource levels on a multidimensional platform. [5]

2.2 *Analysis of past Defending method against Co-residency attack*

Table 1 show the comparatively analysis of existing method that used against Co-residency based Cross-VM attack.

Table 1

Study of existing security method against Cross- VM Side Channel attack

Title	Proposed Solution	Attribute	Objective	Simulation Tool
Sakshi et. al. [6]	MVMP	Metric co-resident success rate	Security	CloudSim
Ahmed et. al.[7]	Secure Algorithm	Metrics Co-Residency based Security	Security	CloudSim
Amit at. Al [8]	PCLF	Performance Metrics	Security	Microsoft Azure
Yuhong Liu et. al. [9]	VM Allocation Strategy	Probability of malicious user	Security	CloudSim
Atul Jia, et. al. [10]	SC-PSSF	Security Risk, CPU, Main Memory	Security	CloudSim

3. Proposed Feathers and Datasets for secure VM allocation

In this research, we will discuss the proposed secure VM placement mechanism in depth. PSO and APSO are two methods that can be utilized to locate the best potential solution for any given systemic function. In addition to this, this is used to indicate how multiple functions will be utilized in order to determine the correct answer. PSO and APSO have been connected to MAS in order to identify attacks that are based on flooding for this planned piece of work. In addition to PSO and APSO,

MAS is utilized in order to collect particles from events for the purpose of verification. PSO and APSO each use their own unique weight functions to check the activities of each node in order to identify any odd variances that may exist between cloud-wide events and event process particles. And the dataset that we are working with is the Distributed Denial of Service (DDoS) attack Evolution dataset that was developed by UNB. This dataset contains information about cloud-based attacks. [9]

3.1 *PSO - Particle Swarm Optimization Detail*

The PSO technique is a population-based stochastic optimization algorithm. It is modelled after the behavior of swarms of birds, swarms of various sorts of insects or ants, or schools of fish, of which the population is referred to as a swarm. If we make the assumption that we represent a function f(X) that generates a actual value out of a vector parameter X (coordinate like (x,y) in a plane), and also that X can start taking on virtually all kind of value in the space for instance, if f(X) is the altitude, so we can discover one for every point in the plane, then we are able to apply particle swarm optimization (PSO). PSO stands for particle swarm optimization. [12] The benefit for parameter X that the PSO algorithm has ascertained to be accountable for generating the least amount of f will be returned by the algorithm (X).

3.2 *Parameters of APSO Used*

Algorithm 1: Algorithm: INITIAL WORK: CLOUD VM EXECUTION

Input : (Create required UB, Region and DC)
Output: Simulation requirment ready for Implement Algorithem 1

Create Userbases and select Region and Calculate the Datacentre based on that
Calculate average cost of (communication / size of data) b/w Datacentre for task to be execute
Setup task node weight W_k as average computation cost per region based on User Base (Handle by Data Centre Broker)
Fix edge weight ek_1, ek_2 as size of file transferred between tasks
for *all task is not scheduled* **do**
    Assign group to user on basis of Algorithm 2
    Data Centre broker will Run LAFwithAPSO for Scheduling (Algorithm 3)
end for
Assign VM their respective task through APSO by UB(Datacentre broker)
Allocate VM for the DC based on APSO Scheduling
Dispatch all the mapped tasks
Check Region for resource of the DC's VM
if *VM's required resource != current DC's Region* **then**
    Update the ready User Base list of Datacentre Broker
    Datacentre Broker will check for all Region for resource
end if
UB will fix the current selected region for DC
After task Completion Datacentre Broker will Destroy executed VM

The initial methodology consisted of merely updating the value to its most recent iteration, which is analogous to restarting the PSO process without reseeding the swarm. Alternately, the function might be reassessed at the place of the individual's best value and then contrasted with the current position. This requires additional function evaluations but has the potential to increase accuracy by preventing the deletion of relevant information. There are multiple possible mechanisms for the sentry [13]. In the beginning, there was a set position that was reassessed after each cycle; however, this did not take into reason the possibility that there could be changes in the nearby area. Using the prior best sites as sentries is one way to circumvent this problem. As a result, we are able to check for changes in a number of different places. [14]

Algorithm 2: Algorithm: Assign DC Group to User

Input : (Request for VM V_i=V_1, V_2, V_3.....V_n)
Output: Assign DC Group to VM

for $U_{current} \leftarrow Vi_n$
do
  if $U_{current}$ *is not in user data* **then**
    Add in default DC Group
    Set threshold value Th_{vlue}
    Check behaviour of $U_{current}$
    if *(Starts VM frequently)* **then**
      $Th_{vlue} \leftarrow Th_{vlue}$ * no of attempts of VM request
    end if
    if *(Start a greater number of VM)* **then**
      $Th_{vlue} \leftarrow Th_{vlue}$ * No of VM Started
    end if
    if *Keeps most of its VM in inactive)* **then**
      $Th_{vlue} \leftarrow Th_{vlue}$ * No of VM Inactive
    end if
    $Th_{vlue} \leq$ SafeTh_{vlue} Move VM to Safe Group
    $Th_{vlue} \geq$ SafeTh_{vlue}
    Move VM to Safe Group
  else
    $U_{current}$ is in user data
    Move to last assign DC Group
  end if
end for

We now propose a placement algorithm called ''Last allocation First (LAF) with APSO (LAF) with the aim of minimizing security risk and maximizing Co-Location Resistance of the cloud.

Algorithm 3: Algorithm: Last allocation First (LAF) with APSO

Input : A list $[t_i]$, $i = 1, 2, \cdots, n$, in T (all task generated by cloudsim) .

Output: Assignment VM to PM on basis of Task $[t_i]$.

```
for all task [t_i] in T(all task generated by cloudsim): do
    Determine t_i to assign task for each VM_i
    Determine t_i allocated to more than one VM(wrong tasks [W_i])
end for
for All Virtual Machine(VM_i) in VM (all initial VM's): do
    Load all VM_i with current allocated t_i
end for
Based on Datacentres (DC) and Userbase (UB) size sort VM (Sorting implimentation)
Based on the Resource Needed to a UB Sort W_i
for all sorted VM_i in VM: do
    for all vm allocated t_i in T : do
        if Real load of VM (K_m) > Current load of VM(K) then
            Schedule task from W_i by calculating best points
            Update value on basis of eq1 and eq2
            Schedule task from DC allocation of VM based on task list best points (P_best)
            Remove allocated task from t_i
            Assign UB for DC allocation of VM based UB resource best points (G_best)
            K++
        else
            Break;
            Load resources based on P_best and G_best
        end if
    end for
end for
return newList
```

Algorithm 2 used to define a category of user is benign or malicious. And after find the category of user put in respective group. Fig 1 show the process of algorithm 2.

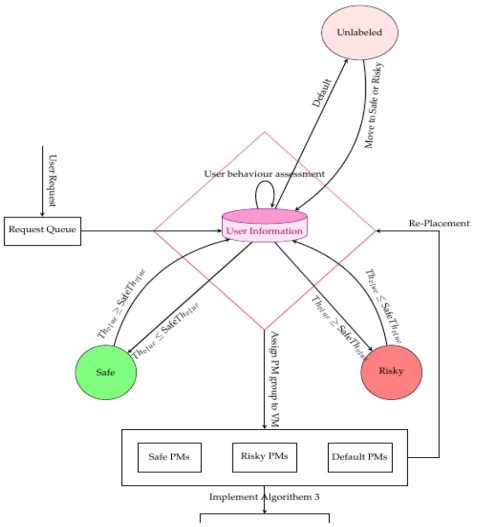

Figure 1

Algorithm 2 flow chart to assign DC group to user

4. Results and experimental evaluation

We do the experiment on CloudSim to demonstrate the usefulness of the LAF (Last allocation First with APSO). We compared the results to other VM allocation algorithms based on ACO. Figure 2(a) shows the comparison among ASP, PSO, and LAF with APSO. In this case, the 10 VMs are hosted in three DCs. In Figure 2(b), 15 VMs are hosted in five DCs.

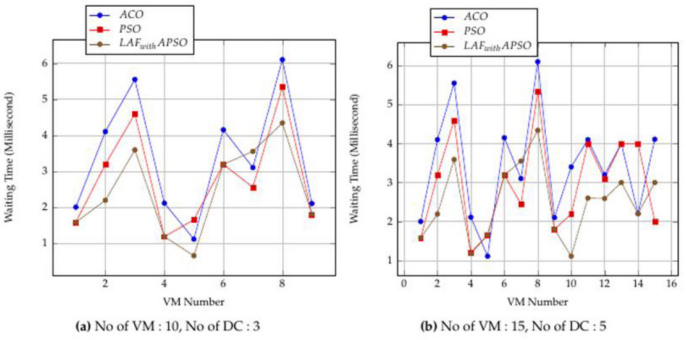

Figure 2

VM placement waiting time comparison in different case

The results of simulation show that the suggested technique is minimize the security risk with considering load and power cost. Figure 3 shows the comparison of virtual machine (VM) co-residency among three different algorithms. This comparison is based on different numbers of users.

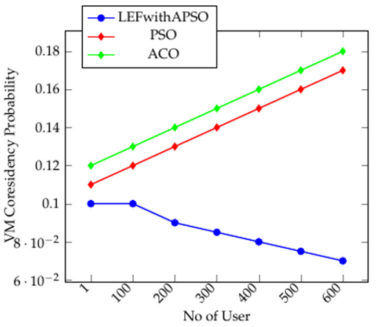

Figure 3

VM Coresidency probability comparison in different case

5. Conclusion

In this article, a co-location based Cross VM based secure VM placement algorithm has been explained that's name 'Last Allocation First (LAF). We describe practically and theoretical analysis of proposed mechanism using CloudSim. Research direction may be classify or identify users (benign or malicious) based on their activity. That will be helpful in security of cloud in future work.

References

[1] Nalini Subramanian and Andrews Jeyaraj. Recent security challenges in cloud computing. *Computers and Electrical Engineering*, 71 : 28-42 (2018). ISSN 0045-7906.

[2] K.E. Narayana and K. Jayashree. Survey on cross virtual machine side channel attack detection and properties of cloud computing as sustainable material. Materials Today: Proceedings, 45 : 6465-6470 (2021). ISSN 2214-7853. International Conference on Mechanical, Electronics and Computer Engineering 2020: Materials Science.

[3] Mengjia Yan, Read Sprabery, Bhargava Gopireddy, Christopher Fletcher, Roy Campbell, and Josep Torrellas. Attack directories, not

caches: Side channel attacks in a non-inclusive world. In 2019 IEEE Symposium on Security and Privacy (SP), pages 888–904. *IEEE* (2019).

[4] Milad Seddigh and Hadi Soleimany. Cross-vm cache attacks on camellia. *Journal of Computer Virology and Hacking Techniques*, 18(2) : 91-99 (2022).

[5] Eswaraprasad, R. and Raja, L., A review of virtual machine (VM) resource scheduling algorithms in cloud computing environment. *Journal of Statistics and Management Systems*, 20(4), pp. 703-711 (2017).

[6] Sakshi Chhabra and Ashutosh Kumar Singh. A secure vm allocation scheme to preserve against co-resident threat. *International Journal of Web Engineering and Technology*, 15(1) : 96-115 (2020).

[7] Ahmed Osama Fathy Atya, Zhiyun Qian, Srikanth V Krishnamurthy, Thomas La Porta, Patrick McDaniel, and Lisa Marvel. Malicious co-residency on the cloud: Attacks and defense. pages 1-9. *IEEE* (2017).

[8] Amit Agarwal and Ta Nguyen Binh Duong. Secure virtual machine placement in cloud data centers. *Future Generation Computer Systems*, 100 : 210-222 (2019).

[9] Yuhong Liu, Xiaojun Ruan, Songjie Cai, Ruiwen Li, and Hanxiao He. An optimized vm allocation strategy to make a secure and energy-efficient cloud against co-residence at- tack. In 2018, pages 349-353. *IEEE* (2018).

[10] Jia, Hefei, et. al. "Security strategy for virtual machine allocation in cloud computing." *Procedia Computer Science* 147: 140-144 (2019).

[11] Varun Natu and Ta Nguyen Binh Duong. Secure virtual machine placement in infrastructure cloud services. In 2017 IEEE 10th Conference on Service-Oriented Computing and Applications (SOCA), pages 26-33. *IEEE* (2017).

[12] Swathi, G., Secure data storage in cloud computing to avoiding some cipher text attack. *Journal of Information and Optimization Sciences*, 39(4), pp.843-855 (2018).

[13] Mohamed A Elshabka, Hanan A Hassan, Walaa M Sheta, and Hany M Harb. Security- aware dynamic vm consolidation. *Egyptian Informatics Journal,* (2020).

[14] Eswaraprasad, Ramkumar, and Linesh Raja. "A review of virtual machine (VM) resource scheduling algorithms in cloud computing environment." *Journal of Statistics and Management Systems* 20, No. 4: 703-711 (2017).