RESEARCH ARTICLE

Multi-Criteria Optimization Based VM Placement Strategy to Mitigate Co-Location Risks in Data Centers

Nelli Chandrakala
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.
kala5136@gmail.com

Vamsidhar Enireddy
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.
vamsidhar@kluniversity.in

Received: 19 June 2022 / Revised: 20 August 2022 / Accepted: 02 September 2022 / Published: 30 October 2022

Abstract – Cloud providers generally run one or more Virtual Machine (VM) instances on the same physical machine. Though it increases data center utilization, it exposes VM to a co-location attack. VM placement and migration are the two strategies adopted for mitigating co-locations. Current methods for VM placement or VM migration consider only security as decision criteria and do not consider other factors like Quality-of-Service degradation, data center utilization, etc. This work proposes a placement and migration strategy for mitigation of co-location attacks with joint consideration of multi objectives like QoS, data center utilization, energy consumption, and security risks. A security-driven multi-criteria optimization -based VM placement policy is proposed. A joint consideration of multi -objective performance optimization along with co-location security risk minimization is done to design a novel VM placement policy based on user categorization. The policy can reduce the likelihood of co-location target VM with attacker VM without much degradation to the performance of VM and data center utilization. The solution mitigates co-location risks without much compromise to the performance of VM and data center resource utilization. The co-residence risk is mitigated by the categorization of users into three levels i.e. unlabeled, risky, and safe, and physical machines into two groups as safe and unsafe. The PMs available in data center is grouped into three different VM placement policies, they are undecided pool, safe pool and unsafe pool.

Index Terms – Cloud security, VM migration, Mitigation of co-location, Data center utilization, Service degradation.

1. INTRODUCTION

Infrastructure as a Service (IaaS) is a cloud computing model where computing, storage, and network resources are offered on demand in units of virtual machine (VM). VM is an abstraction of a physical machine (PM) with facilities for resource provisioning on demand. Consumers rent out VM from the cloud service providers. These providers often use the same physical machine to run multiple VM depending on the capacity of the physical machine. These VM residing in the same physical machine are called co-location VM. The co-location VMs share the same hardware resources but logical isolation is provided by a virtualization component called a hypervisor. Though co-location improves the resource utilization of the physical machine, it poses a serious security threat when at least one VM is an attacker. The attacker VM can break the logical isolation and access the memory and network contents of any other VM for any malicious purpose. The problems due to co-location attacks are studied in detail several works [1-2]. The attacker VM can launch various attacks like side-channel [3], memory DOS [4], etc. The first and foremost reason for co-location attacks is the placement of VM without any constraints or violation checks. The attacker gains knowledge about the placement policies in the cloud and uses it to get the attacker VM gets placed in the same physical machine as the target VM. Existing VM placement policies are based on certain optimization constraints like maximizing resource utilization, minimizing energy etc. So, an attacker can queue in his requests right next to or immediate vicinity to target VM requests, so that there is a higher probability of co-location of the target VM and attacker VM. Co-location can also occur during VM migration. Attackers generally observe the placement patterns and launch VM requests for maximizing the likelihood of co-location of attacker VM and target VM. There are many existing works proposed for mitigation of co-location attacks categorized as attack-specific defenses [5-6], modifications in OS system calls [7], hypervisor adaptations

[8], hardware modifications [9], etc. These approaches degrade the performance of the applications running on VM. The solution for mitigation of co-location attacks without much performance degradation is in adaptations to VM placement and migration policies. Both VM placement and migration process must be adapted for joint consideration of multi-objective optimization like QoS, utilization, energy consumption, and co-location security risk. In this way, co-location likelihood can be reduced without much degradation to performance factors [10].

An Evolutionary Quantum Neural Network (EQNN) constructed capability calculation method for Cloud datacenter activities and computational productivity of significant computation by encrypting capability information into qubits and broadcasting this information over the network to estimate the capacity with higher precision [11]. Protected joint validation is an essential necessity to share structural vital information between collaborating units in the merged cloud security. A joint validation technique that includes a machine learning-based collaborative voting classifier for online threat finding and Elliptic Curve Cryptography signature scheme-based agreement to confirm safe communication among the sharing units [12]. In existing methods, the VMs are allocated to physical servers based on-demand. This method is modest but it results in a deprived performance due to source destruction. The productivity of a data center therefore depends on provisioning and placement of VMs. The proper placement scheme will improve the quality of service and decrease the operation cost of the data center [13]. Ineffective VM placement causes to high-power consumption that increases the necessity for server alliance. To offer the exact solution of the multi-objective and multi-constrained VM allocation problems, and accomplish effective server consolidation the GA based evolutionary server consolidation framework is presented [14]. The cloud computing supports digitization all over the world and offers a collective pool of resources, available from anywhere, at any time and distributed on request as a service [15]. The regular variations in a cloud user's supply causes an additional power consumption, wastage of resource. These challenges are addressed and consolidated the entire load on the least number of energy-efficient physical machines [16].

1.1. Research Gap

Most of the existing solutions for mitigation of co-location attacks are based on limiting the number of users in a server or grouping the users and restricting VM of that user group to server. But these approaches can cause severe degradation to resource utilization when scaled to large data centers. This necessitates a scalable VM placement policy to be designed with joint consideration of security, VM performance and data center utilization. The security-aware VM allocation policy needs to developed that aims to assign the VMs securely and decreases the probable co-residency between hateful and target VMs

1.2. Motivation of the Research

The current methods discussed in related works for VM placement or VM migration consider only security as decision criteria and does not consider other factors like quality-of-service degradation, data center utilization etc. To prevent the chances of attacker and target VM co-location as user characteristics, there is a need to provide a detailed security -driven multi - criteria optimization -based VM placement policy to assign the VMs securely and to decrease the probable co-residency between hateful and target VMs; this motivates to propose the following work.

1.3. Contributions

This work contributes a placement and migration strategy for mitigation of co-location attacks with joint consideration of multi objectives like QoS, data center utilization, energy consumption, and security risks. A security - driven multi - criteria optimization -based VM placement policy is proposed. The joint consideration of multi - objective performance optimization along with co-location security risk minimization is done to design a novel VM placement policy based on user categorization. This policy is able to reduce the likelihood of co-location target VM with attacker VM without much degradation to the performance of VM and data center utilization. The solution also mitigates co-location risks without much compromise to the performance of VM and data center resource utilization.

1.4. Organization of Paper

The paper is organized as follows. This section of the paper had a brief introduction on solution for mitigation of co-location attacks, existing VM placement policies, research gap, motivation and contributions of the research. Section 2 reviews the existing literature related to co-location VMs and VM placement strategies. Further, it compares the different attacks and mitigation methods. Section 3 describes the proposed security driven multi criteria optimization with three objectives of reducing the co-location risks, scheduling optimal resources to VM and reducing the distortion to data center utilization. Section 4 describes the result analysis. Section 5 concludes this paper.

2. RELATED WORKS

Xin Liang et al [17] addressed the grouping based VM location approach to mitigate co-location attacks. But the grouping based VM placement approach is not safe when attacker launches multiple VM requests spread in a uniform time interval. Amit Agarwal et al [18] proposed a VM location algorithm called "Previously Co-located users First". This approach categorizes the users to two types: new user and already known user. New user VM' are placed randomly but known users VM are co-located with already co-located VMs. This approach gives higher reputation to already known user and doubts only new users for any foul play. Yuqin Qiu, et al [19] projected a co-residency resistant VM placement policy. Authors proposed two metrics: VM co-residency possibility and user co-residence coverage chance to evaluate the placement policy. The deployment policy is dynamic and it is selected in way to reduce VM co-residency possibility. The number of users on particular host is controlled to mitigate co-residency attacks. Mouhebeddine Berrima et al [20] proposed a VM placement strategy by negotiating the VM startup time. All incoming requests for VM are queued up. Only when the queues are filled up, the VM are assigned to random servers. By this way co-location probability can be reduced. Varun Natu et al [21] proposed a VM placement solution based on trust profile of VM. User specifies the security limitations in terms of reliable parties or other users for co-location. Cloud providers provide the list of users and their trust reputation scores for each user to calculate their trust set. The VMs is scheduled to physical machine within the constraints of trust set. Yi Han et al [22] proposed a VM placement strategy called previously selected servers first (PSSF). The solution reduces the average number of users per server. The VM created by the user is allocated to servers which previously hosted the VM. In case those servers are unavailable, a server with least number of VM is preferred. Mansour Aldawood et al [23] proposed a security aware VM allocation algorithm to mitigate co-location attacks. The algorithm is a variant of bin packing with goal of minimizing VM migrations and reduced the number of PMs with co-residency. Yi Han et al [24] classified the users into three types of: low, medium and high risk based on their past behaviors. VM belonging to same types only can be co-located. By this way, it becomes tough for attackers to co-locate with target VM unless their credibility is proved. Deepika Saxena et al [25] projected a safe and multi objective VM location algorithm. A hybrid meta-heuristic based on combination of whale optimization and genetic algorithm is used to select the most optimal VM placement policy. The security for physical machine is evaluated in terms of number of different users allocated on same server. Optimization algorithm tries to minimize it and compensate for the performance degradation by balancing the VM across the available physical machines to increase utilization. Sakshi Chhabra et al [26] used the policy of not allocating different user VM on same physical machine to mitigate co-location attacks. The VM are always allocated to new servers and evaluated using intrusion detection systems before placing to another VM. Vu Duc Long et al [27] proposed group instance placement technique to deal with co-residency attacks. Cloud users are organized into groups by the cloud service provider. The physical machines are allocated VM only from the group instance. By controlling the users in group and size of group, it becomes tough for attackers to co-locate with target VM unless he is in same group set. The effectiveness of the algorithm depends on how group instance is formed. Nguyen Binh Duong et al [28] proposed a secure VM provisioning algorithm for enterprise users. Users are grouped based on the work sensitivity. VM's of users across different group are not allocated to same host. Based on the number of users in each group, the hosts are provisioned [29]. With the fast development of the technological advancements, and the growing number of cloud users, a model renovation to separate data and control point is taking place [30].

The current methods discussed in related works for VM placement or VM migration consider only security as decision criteria and does not consider other factors like Quality-of-Service degradation, data center utilization etc. To improve security issues and to prevent the chances of attacker and target VM co-locating as user characteristics. The extension of the work is proposed a placement and migration strategy for mitigation of co-location attack with joint consideration of multi objectives like QoS, data center utilization, energy consumption and security risks. The comparison of different attacks and mitigation methods are given in table 1.

Table 1 Comparison of Different Attacks and Mitigation Methods

Existing Works	Parameter	Attack names	Methodologies	Conclusion
Mitigating Cloud Co-Resident Attacks [17]	Cloud Co-resident Attacks	Cross-VM attacks, such as side channel attacks or memory Dos attacks,	Grouping-based VM placement strategy	This strategy is more effective in terms of both co-location resistance and resources efficiency.
Co-Location Resistant Virtual Machine Placement [18]	Co-location resistance	Cross-virtual machine (VM) side-channel attacks, the security of public IaaS cloud data centers	"Previously Co-Located Users First" (PCUF)	In this approach handles the initial VM placement problem, open challenges with the target user during initial VM placement

A Secure Virtual Machine Deployment Strategy [19]	Reducing co-residency	Side channel attacks and covert channel threats.	Co-residency-resistant VM deployment strategy	Get better security and load balancing performance
Co-location Resistant Strategy [20]	Co-location resistance	The attack against the integrity, confidentiality or availability.	Secure-optimal placement algorithm	This strategy allows to decline the probability of co-location with start-up delay.
Virtual Machine Allocation Policies [22]	Cloud Co-Resident Attacks	Co-resident attack	Virtual Machine Allocation Policies	Proposal of new policy that mitigates the threats and satisfies the workload balance problems
Placing Virtual Machines Securely in Cloud Environments [23]	Secure Placement of Virtual Machines	Malicious co-residency between VMs.	SRS algorithm	Development of a secure VM allocation algorithm to decrease the potential for co-residency between malicious and target VMs.
A secure VM allocation scheme [26]	Co-resident threat	co-resident attacks	Virtual machine allocation policy (MVMP)	Mitigation of the threats by reducing the possibility of attackers co-locating with the targets
Group Instance: Co-Location virtual machine placement [27]	Co-Location Resistant	Co-location attacks	Group instance to deal with co-location attacks	Proposal of algorithm for co-location resistant VM placement that can accomplish improved performance
Handling Co-Resident Attacks [28]	Co-residency attacks	Co-residency attacks	Secure and cost-effective VM provisioning methods	In this work, the possible cost-effective and secure methods are proposed to provide security when security groupings are not available.

3. SECURITY DRIVEN MULTI CRITERIA OPTIMIZATION

The proposed security driven multi criteria optimization (SD-MCO) is designed with three objectives of reducing the co-location risks, scheduling optimal resources to VM and reducing the distortion to data center utilization. The architecture of the SD-MCO is given in Figure 1. The core of the solution is VM placement based on category of users requesting it. The solution categorizes user to three classes: un-labeled, safe and risky. Three different VM placement strategies are proposed to handle the three classes of users. Initially all the users are un-labeled and they are categorized to safe or risky based on their behavior over time using sequential probability test. The physical machines are grouped into three categories of undecided, safe and unsafe. The VM can be placed with full optimization of resources matching the VM performance needs within the safe group. Initially, the number of PMs in safe group is less compared to unsafe and undecided group. But as more users are moved to reliable category proportional number of PM's are moved to safe group from unsafe group. For un-labeled user, VM are placed using random selection policy. For reliable users, VM's are placed using multi criteria optimization on safe category of PM's. For risky. users, VM's are placed with spread based allocation policy on unsafe category of PM's. Users whose VM's are allocated in unsafe category are continuously evaluated for their behavior and this incurs some extra cost. This cost is initially high, but as the credibility of users is proved and more users are moved from category of unlabeled to reliable or risk, this cost is reduced. Following are three core functionalities of the proposed solution

- Categorization of users
- Scheduling for different categories of users
- PM grouping

These functionalities are explained in detail in below sections.

3.1. Categorization of Users

A three-state model with transition triggered based on sequential probability test is proposed in this work. The users are categorized based on the behavior of the user VM dynamics in undecided

PM's. Users are initially in unlabeled state. User characteristics for reliable and risk state is given in Table 1.

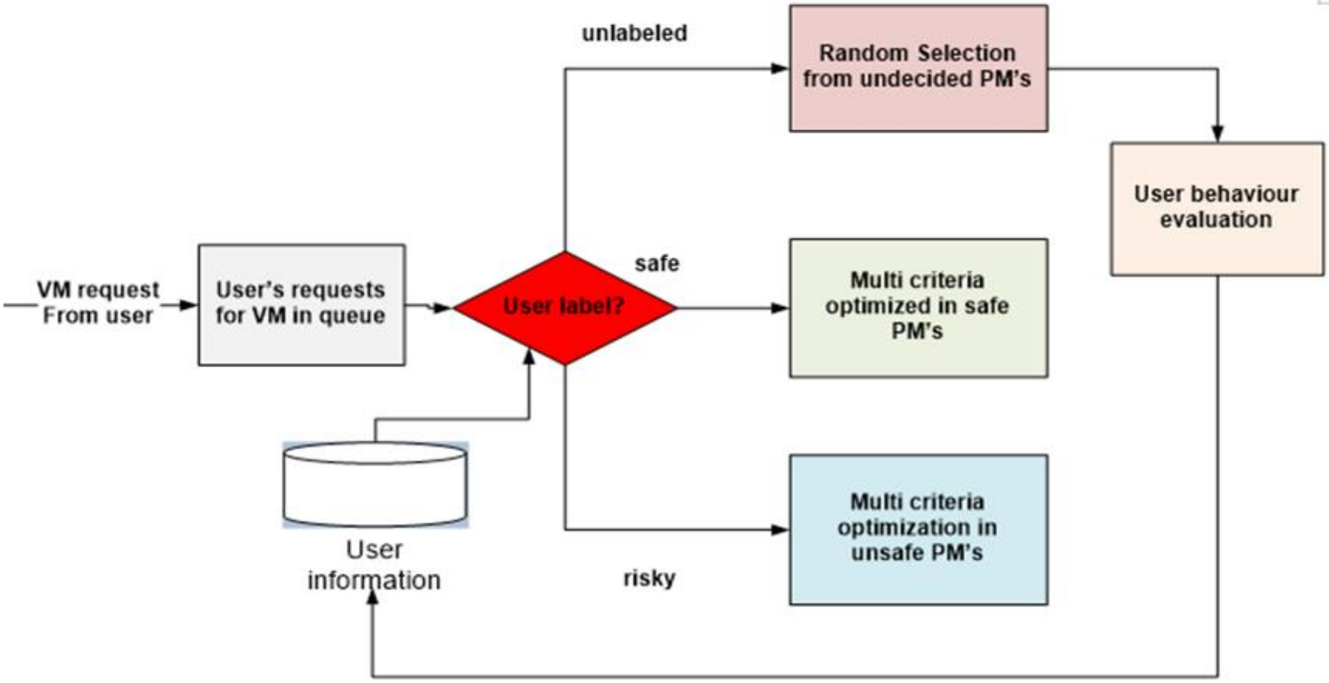
unlabeled
Random Selection from undecided PM's
User behaviour evaluation
safe
VM request From user
User's requests for VM in queue
User label?
Multi criteria optimized in safe PM's
User information
Multi criteria optimization in unsafe PM's
risky

Figure 1 Architecture of SD-MCO

Table 2 User Characteristics

User	Characteristics
Undecided	Default
Attacker	Start considerably a greater number of VM Starts VM frequently Stays active once it co-resides in its target VM Keeps most of its VM in inactive cost to reduce the cost
Not attacker	When user is not decided as Risky through sequential probability test.

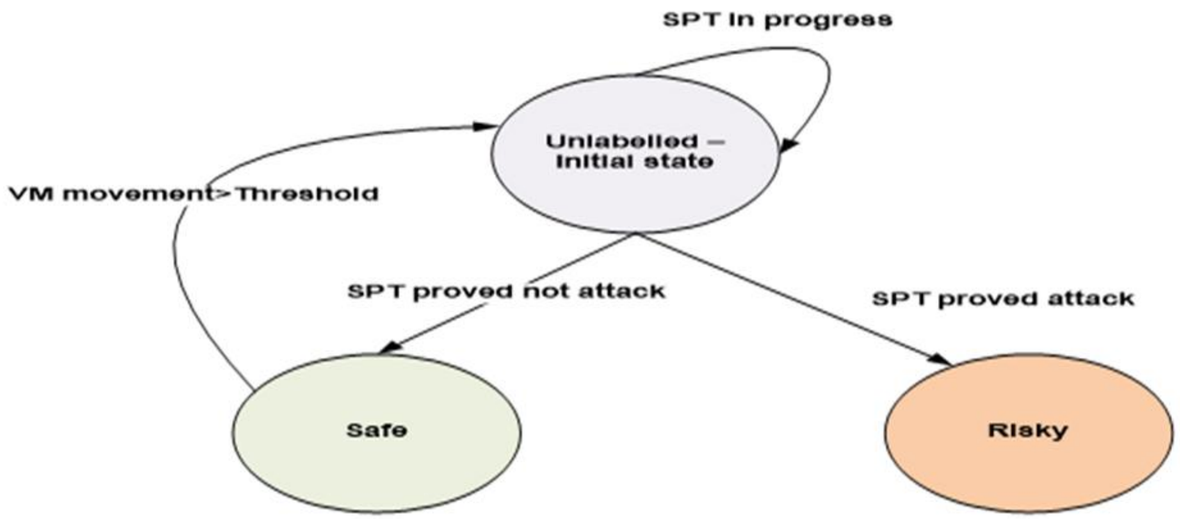

Figure 2 User State Transition

The state transition among these three states is demonstrated in Figure 2. Initially user is in undecided state. Sequential probability test (SPT) is launched in un-decided state to check for attack characteristics listed in Table 1. Sequential probability test [23] is launched on VM dynamics to assess the trustworthiness of user. The sequential probability test (SPT) is an essential tool for sequential study. It develops the foundation of several successive techniques for diverse applications.

Sequential probability test tries to prove one of the following hypotheses

H0: Observed user is attacker

H1: Observed user is not attacker

To prove the hypothesis this work uses two thresholds A, as shown in equation (1) (upper) and B, as shown in equation (2) (lower) based on false positive rate α and false negative rate β as follows

$$A = \log \frac{\beta}{1-\alpha} \qquad (1)$$

$$B = \log \frac{1-\beta}{\alpha} \qquad (2)$$

The tolerant value for β is set by the user information system.

The log probability for an observed user x for T tests is given as shown in equation (3),

$$P(x) = \log \frac{\prod_{t=1}^{T} P_1(S_t)}{\prod_{t=1}^{T} P_0(S_t)} \qquad (3)$$

Based on P(x) following observations can be done. Here P1 denotes probability under the hypothesis

St discrete or continuous probability density function

Hypothesis H0 can be accepted if $P(x) < A$ and the test can be stopped for the observed user x.

Hypothesis H1 can be accepted if $P(x) > B$ and the test can be stopped for the observed x.

For $< P(x) < B$, both of the hypothesis cannot be confirmed now and further test is needed for verifying if the observed user x is attacker.

If SPT confirms user is attacker, user is labeled as risky. If SPT confirms user is not attacker, user is labeled as safe. However, when number of VM movements in a period of time, triggered by user switching on and off the VM is above certain threshold, then reliability is user is doubted and user is moved back to undecided state.

3.2. Scheduling of Different Category of Users

Three different scheduling policies are proposed for three categories of users. Unlabeled users request from different users are taken from queue and random shuffling of requests is done to create a mix order. Till N requests are piled up, the VM's are not taken for placement. VM's are taken randomly from the queue and placed on the random server in the undecided PM group. Attackers usually exploit the temporal correlation of target users VM and give their request in same time or with small difference, so that there is a maximum likelihood of placement on same physical machine. But queuing N requests, creating mix order and pickup random from queue can introduce large delay in processing between target user and attack user requests.

This scheduling prompts the attack user to do trigger rescheduling to target VM 's server by switching off and on the VM till it achieves success. This behavior is captured by SPT to detect the user as attacker.

The probability of detecting risky user is modeled in terms of size of queue N. In the queue, there can be $N_a$attack users, N_t target users and N_o other users by adapting the model proposed in [14]. The number of attacked users on k^{th}server is given as shown in equation (4),

$$NA = \frac{p.N_t^k}{N^k}.(1 - \frac{\binom{N+N_o^k-1}{p-1}}{\binom{N^k-1}{p-1}} \qquad (4)$$

From NA , the probability of detect risk user is calculated by using the equation (5),

$$P_d = \frac{NA}{Number\ of\ users\ in\ the\ queue} \qquad (5)$$

Other users: Both risky and safe users are allocated using same multi criteria optimization policy except that risky users are allocated in unsafe PM's and safe users are allocated in safe PM's. The VM's must be placed in the PM's satisfying following three constraints.

Table 3 Constraints

Assignment	Each VM must be allocated sufficient resources to satisfy service level agreements
Capacity	The VM must be fit within the capacity of the PM
Placement	VM is placed only on one server

The VMs must be placed in the PMs in such way to satisfy multiple objectives of: maximize total utilization of individual PMs, reduce the overall energy consumption,

The utilization of PMs is calculated in terms CPU utilization is as shown in equation (6),

$$U_i = \frac{\sum_{q=1}^{|R|}\sum_{i=1}^{|RqVM|} R_q.VM_i.C.CPU \times R_q.VM_i.B}{U_{i.}.CPU} \qquad (6)$$

Where R is requests within a interval. R_qVM is the number of VM demands in a request R_q. $R_q.VM_i.C.CPU \times R_q$are the CPU cycles needed for R_qVM. $R_q.VM_i.B$ has two values of 0 or 1 depending on whether VM is placed in the server or not.

The total utilization is calculated by using the equation (7),

$$U = \sum_{i=1}^{|PM|} U_i \qquad (7)$$

The energy consumed in PM is calculated by using the equation (8),

$$e_j = \left(e_j^{max} - e_j^{idle}\right) \times U_j + e_j^{idle} \qquad (8)$$

The total energy consumption is calculated by using the equation (9),

$$E = \sum_{i=1}^{|PM|} e_i \qquad (9)$$

The VM's must be placed in PM using the following objective function as shown in equation (10),

$$FF = minimize(\frac{\sum_{i=1}^{|PM|} e_i}{U}) \qquad (10)$$

The solution to problem of placing the VM to the PM with minimization of E subject to constraints given in Table 2, is a NP hard problem. In this work the Particle swarm optimization to provide a heuristics solution to this problem is used. The PSO is a swarm intelligence algorithm simulating the social behavior of swarm of organisms. This technique is common for resolving optimization complications due it its easiness and adaptability. Organisms transfer arbitrarily with diverse velocities and use these velocities to apprise their separate location. Each contender result is a 'particle'. Each particle attempts to accomplish its finest velocity based on its individual local best (p_{best}) value and its neighbor's comprehensive best (g_{best}). Each particle's successive location be contingent on the present location, present velocity, distance from existing location to p_{best}, distance from present location to g_{best}. The transfer of particle in its search space based on its velocity. For a particle X, its present location $X_i$and present velocity V_i is updated as shown in equation (11) and (12) respectively,

$$X_i(t+1) = X_i(t) + V_i(t+1) \qquad (11)$$

$$V_i(t+1) = wV_i(t) + c_1r_1\left(p_{besti}(t) - X_i(t)\right) + c_2r_2\left(g_{besti}(t) - X_i(t)\right) \qquad (12)$$

In equations (11) and (12), t is the iterative value. c_1 and c_2 are acceleration coefficients,.r_1 and r_2 are random numbers, w is the inertia weight. The iteration is repetitive till end state is met.

Let m be the number of particles and n is the number of dimension space of the particle. Each PM is treated as particle each VM is denoted as a dimension element of the particle. The i^{th} particle at iteration t is denoted as $X_i^t = (x_{i1}^t, x_{i2}^t, \dots x_{in}^t)$ where $x_{ix}^t \in (0,1)$ with 1 indicating VM is placed on the PM and 0 indicating VM is not placed on the PM. Initially random solution m particles are formed (m random solutions for VM placement). Fitness is calculated for each particle. Individual best position and global best position are adjusted with value of fitness function FF. The particle $((X_i(t+1))$and speed of particle $(V_i(t+1))$ are adjusted based on p_{best} and g_{best}.

When PSO algorithm converges, meeting the termination criterion, the approximate solution for placement of VM onto corresponding PM satisfying the multi objectives and constraints is got as result. The above PSO optimization algorithm is implemented for placing unsafe users VM in unsafe PMs. Another instance of PSO optimization algorithm is used for placing the safe users VM in safe PMs. Where the particle $((X_i(t+1))$and speed of particle $(V_i(t+1))$ are the multi-objective functions

3.3. PM Grouping

The PMs available in data center is grouped into three categories of undecided, safe and unsafe PM's. Initially maximum number of VM is kept in undecided pool. When users are marked as unlabeled to safe, the PM capacity needed to accommodate the VM allowed for user is added to sage pool. Similarly, when users are marked as unlabeled to risk, the PM capacity needed to accommodate the VM allowed for user is added to unsafe pool. When user is moved from safe to unlabeled, corresponding PM capacity is returned to undecided pool.

4. RESULT ANALYSIS

The proposed SD-MCO solution is simulated in Cloudsim. The simulation is done with the configuration shown in table 4.

The performance of the SD-MCO is verified in terms of: VM co-residency probability, user's co-residency coverage probability, data center utilization and energy consumption. The efficiency of the probable SD-MCO is equated in contradiction of security attentive VM distribution algorithm (SRS) [23], secure multi objective virtual machine placement (SM-VMP) [25] and group instance based flexible co-location resistant virtual machine location (GI) [27]. The group instance (GI) virtual machine (VM) location method is to handle co-location attacks in public Infrastructure-as-a-Service (IaaS) clouds. Definitely, the group instance classifies cloud users into clusters with different magnitudes set by the cloud provider. The SRS security-aware VM distribution algorithm (SRS) that purposes to assign the VMs securely and to decrease the probable co-residency among hateful and target VMs.

Table 4 Simulation Configuration

Parameter	Values
Number of PM	500
Host configuration	20 GB RAM,100GB disk space, 30 CPU cores
Number of users	500
Number of target user	10%
Number of attacker user	20 %

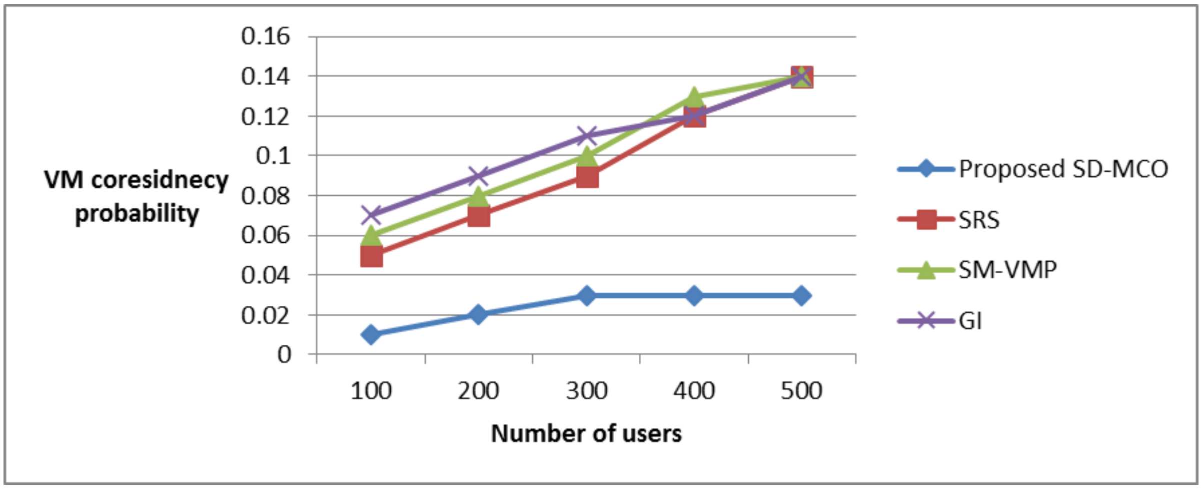

Figure 3 VM Co-Residence Probability

The results for VM co-residence probability between attacker and target VM is determined for various users and the outcome is shown in Figure 3. The typical VM co-residence probability in proposed SD-MCO is 0.024, SRS is 0.094, SM-VMP is 0.102 and GI is 0.016. The VM co-residence probability is almost 2 times lower than existing works. The VM co-residence probability is almost same across number of users and comparatively lower than existing works in proposed solution. The co-residence probability has reduced in proposed solution due to three level categorization of users and continuously evaluating the users using SPT. The existing algorithm limits the number of users to server achieve lower co-residence probability, but with probability of any user can become attackers, the co-residence probability increases.

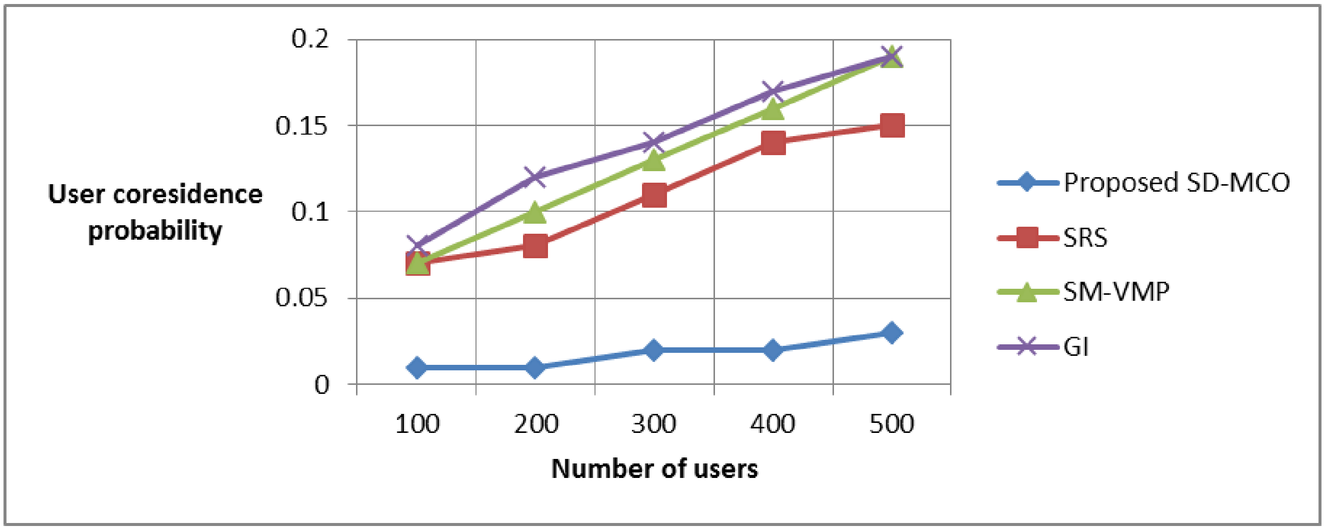

Figure 4 User Co-Residence Probability

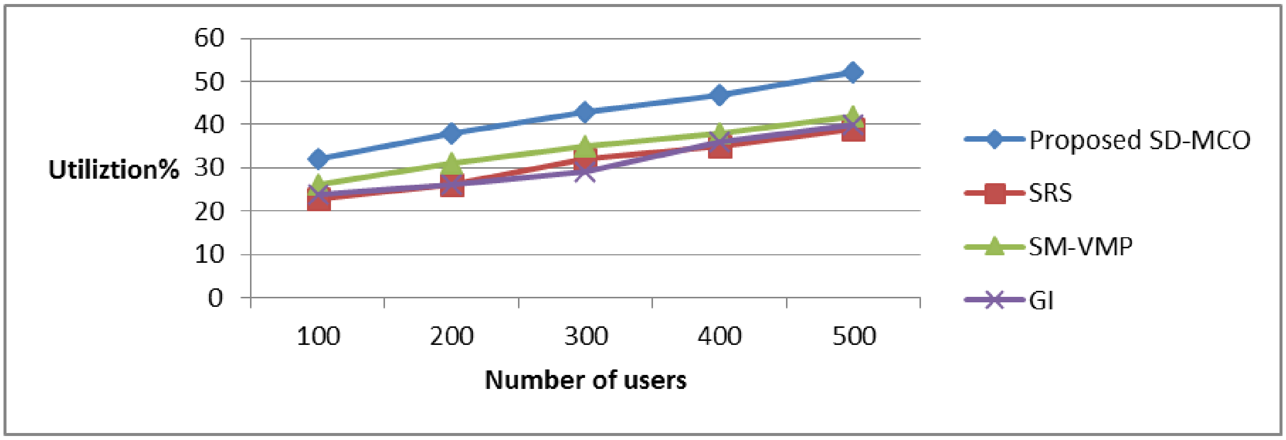

Figure 5 Data Center Utilization

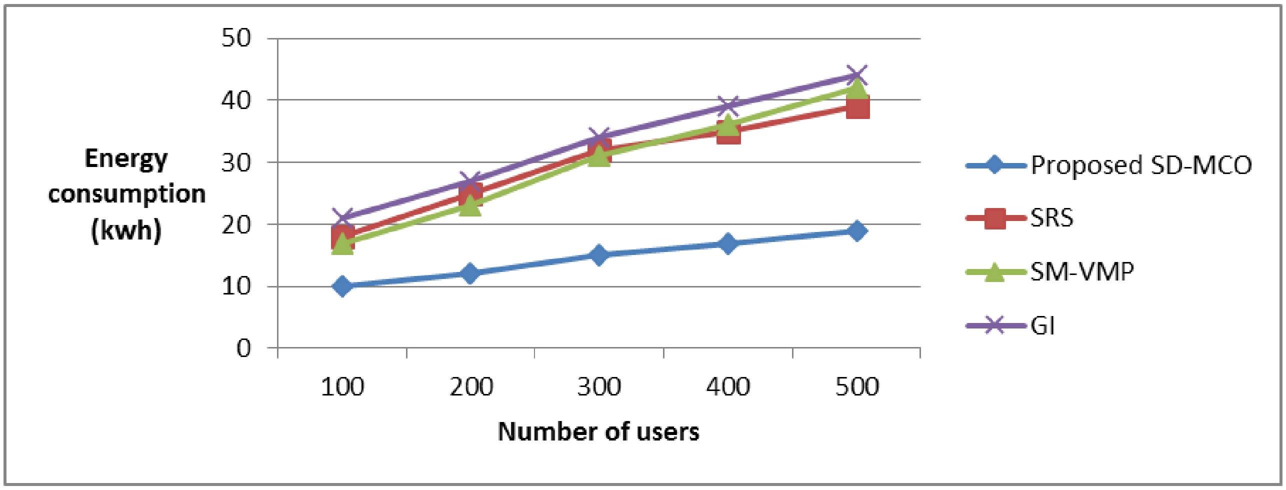

Figure 6 Energy Consumption

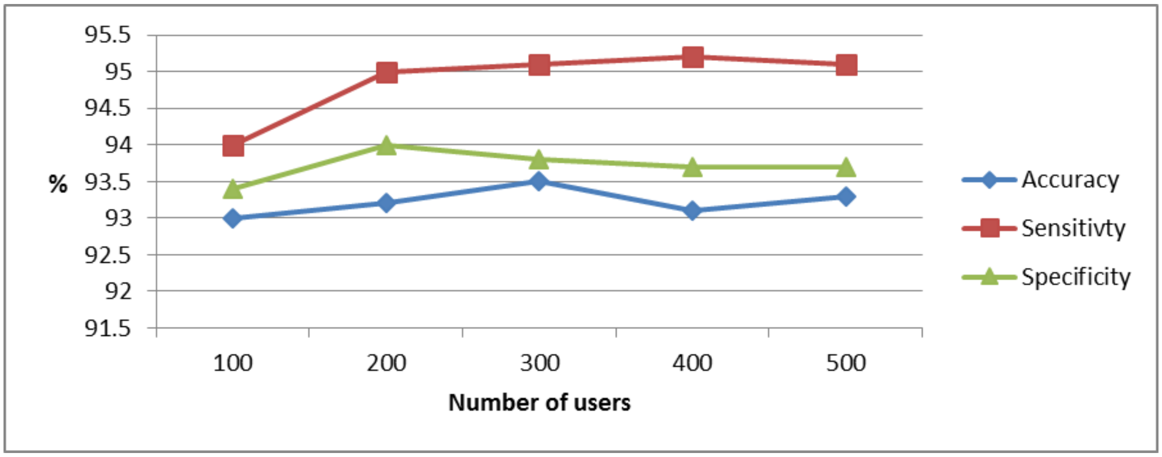

Figure 7 SPT Performance

The user co-residency coverage probability between attacker and target user is calculated for different users and the outcome is shown in Figure 4. The average user co-residence probability in proposed SD-MCO is 0.018, SRS is 0.11, SM-VMP is 0.13 and GI is 0.14. The user co-residence between attack and target user is very low due to SPT. SPT is able clearly move attacker user to unsafe PM pools thereby co-residence becomes difficult. However, in absence of much attack characteristics, SPT is able to detect attacker user and these leaks as small fraction of co-residence in proposed solution.

The data center utilization among the VM allocated PM's is measured for different number of users and the result is given in Figure 5. The average data center utilization is proposed solution is 11.4% higher compared to SRS, and 8% higher compared to SM-VMP and 11.4% compared to GI. The utilization has increased in proposed SD-MCO due to relaxation of the condition of allocating only same users to the VM. But existing works were not able to increase the utilization due to this condition. Also, the consideration of multi criteria optimization with maximizing utilization as criteria have increased the data center utilization is proposed solution.

The energy consumption is measured for several number of users and the outcome is shown in Figure 6. The typical energy consumption is at least 2 times lower in proposed SD-MCO related to existing works. The reduction is due to multi criteria optimization in both safe and unsafe PM pools leading to better placement of VM to PM without any restriction limiting users in the server. The accuracy, sensitivity and specificity of detecting co-location attacker using SPT for various users is measured and the outcome is shown in Figure 7. The average accuracy of attacker detection in proposed solution is 93.22%. The sensitivity is 94.88% and specificity is 93.72%. With the considered attacker characters the proposed solution is able to detect attacker user and able to isolate him from other VM's with an accuracy of 93.22%.

5. CONCLUSION

A security driven multi criteria optimization based VM placement strategy is proposed in this work. The solution mitigates co-location risks at same time achieve without much comprise to performance of VM and data center resource utilization. The co-residence risk is mitigated by categorization of users to three levels and physical machines to two groups. Three different VM placement policies are proposed for handling VM requests from three users. The proposed solution was found to provide better resource utilization and lower co-location risk compared to existing works. The proposed solution is also able to scale well for large data centers. The performance was tested by using Cloudsim simulation tool. The movement of PM to safe and unsafe group can be triggered based on arrival rate of VM's from different categories of users can be extended as future work.

REFERENCES

[1] Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan 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, DOI.org/10.1145/1653662.1653687.

[2] Yinqian Zhang, Ari Juels, Michael K. Reiter, Thomas Ristenpart, "Cross-vm side channels and their use to extract private keys",Proceedings of the 2012 ACM conference on Computer and communications securitys, pp. 305-316, 2012.DOI.org/10.1145/2382196.2382230.

[3] Abid Shahzad, Alan Litchfield, "Virtualization Technology: Cross-VM Cache Side Channel Attacks make it Vulnerable", Presented at the Australasian Conference on Information Systems, pp.1-16, 2016, DOI.org/10.48550/arXiv.1606.01356.

[4] Tianwei Zhang, Yinqian Zhang, Ruby B. Lee, "Memory dos attacks in multi-tenant clouds: severity and mitigation," arXiv preprint: 1603.03404, 2016.

[5] Soo-jin Moon, Vyas Sekar, Michael K. Reiter, "Nomad: mitigating arbitrary cloud side channels via provider-assisted migration",

Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15), pp. 1595-1606, 2015, Doi.org/10.1145/2810103.2813706.

[6] Jingzheng Wu, Liping Ding, Yuqi Lin, Nasro Min-Allah, Yongji Wang, "Xenpump: a new method to mitigate timing channel in cloud computing", IEEE Fifth International Conference on Cloud Computing (CLOUD '12), pp. 678--685, 2012, DOI: 10.1109/CLOUD.2012.28.

[7] Yinqian Zhang, Michael K. Reiter, "Düppel: retrofitting commodity operating systems to mitigate cache side channels in the cloud", Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13), pp. 827-838, 2013, Doi.org/10.1145/2508859.2516741.

[8] Taesoo Kim, Marcus Peinado, Gloria Mainar-Ruiz, "Stealthmem: system-level protection against cache-based side channel attacks in the cloud", Proceedings of the 21st USENIX conference on Security symposium (Security'12), pp. 189-204, 2012, Doi/10.5555/2362793.2362804.

[9] Michael Godfrey, Mohammad Zulkernine, "Preventing cache-based side-channel attacks in a cloud environment", IEEE Transactions on Cloud Computing, volume. 2, no. 4, pp. 395-408, 2014.

[10] Adi Fuchs, Ruby B. Lee, "Disruptive prefetching: impact on side-channel attacks and cache designs", Proceedings of the 8th ACM International Systems and Storage Conference (SYSTOR '15), pp.1-12, 2015, DOI:10.1145/2757667.2757672

[11] Ashutosh Kumar Singh, Deepika Saxena, Jitendra Kumar, Vrinda Gupta, "A quantum approach towards the adaptive prediction of cloud workloads", IEEE Transactions on Parallel and Distributed Systems, volume. 32, no. 12, pp. 2893-2905, 2021.

[12] Ashutosh Kumar Singh, Deepika Saxena, "A cryptography and machine learning based authentication for secure data-sharing in federated cloud services environment", Journal of Applied Security Research, volume. 17, no.3, pp. 385-412, 2021.

[13] Thuan Duong-Ba, Tuan Tran, Thinh Nguyen, Bella Bose, "A dynamic virtual machine placement and migration scheme for data centers", IEEE Transactions on Services Computing, volume. 14, no. 2, pp. 329-341, 2021.

[14] Deepika Saxena, Ashutosh Kumar Singh, "Energy aware resource efficient-(EARE) server consolidation framework for cloud datacenter", Proceedings of ICACCT, Advances in Communication and Computational Technology pp. 1455-1464, 2021, DOI:10.1007/978-981-15-5341-7_111.

[15] Deepika Saxena, Ashutosh Kumar Singh, "Communication cost aware resource efficient load balancing (CARE-LB) framework for cloud datacenter", Recent Advances in Computer Science and Communications, volume. 14, no. 9, pp. 2920-2933, 2021.

[16] Deepika Saxena, Ashutosh Kumar Singh, "A proactive autoscaling and energy-efficient VM allocation framework using online multi-resource neural network for cloud data center", Neurocomputing, volume. 426, pp. 248-264, 2021.

[17] Xin Liang, Xiaolin Gui, Jian, A Jian, Dewang Ren, "Mitigating cloud co-resident attacks via grouping-based virtual machine placement strategy", IEEE 36th International performance computing and communications conference (IPCCC), pp.1-8, 2017, DOI:10.1109/PCCC.2017.8280448.

[18] Amit Agarwal, Ta Nguyen Binh Duong, "Co- Location Resistant Virtual Machine Placement in Cloud Data Centers," IEEE 24th International conference on parallel and distributed systems (ICPADS), pp. 61-68,2018. DOI: 10.1109/PADSW.2018.8644849.

[19] Yuqin Qiu, Qingni Shen, Yang Luo, Cong Li , Zhonghai Wu,"A secure virtual machine deployment strategy to reduce co-residency in cloud," IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 347– 354, 2017. DOI: 10.1109/Trustcom/BigDataSE/ICESS.2017.257

[20] Mouhebeddine Berrima, Aïcha Katajina Nasr, Narjes Ben Rajeb, "Co-location resistant strategy with full resources optimization," in Proceedings of the 2016 ACM on Cloud Computing Security Workshop, pp. 3–10,2016, DOI.org/10.1145/2996429.2996435.

[21] Varun Natu, Ta Nguyen Binh Duong,"Secure virtual machine placement in infrastructure cloud services," IEEE 10th Conference on Service-Oriented Computing and Applications (SOCA) pp. 26–33, 2017, DOI: 10.1109/SOCA.2017.12

[22] Yi Han, Jeffrey Chan, Tansu Alpcan,Christopher Leckie, "Using virtual machine allocation policies to defend against co-resident attacks in cloud computing", IEEE Transactions on Dependable and Secure Computing, volume. 14, no. 1, pp. 95–108, 2017.

[23] Mansour Aldawood, Arshad Jhumka, Suhaib Fahmy, "Sit Here: Placing Virtual Machines Securely in Cloud Environments", Proceedings of the 11th International Conference on Cloud Computing and Services Science - CLOSER, pp.248-259, 2021, DOI:10.5220/0010459202480259.

[24] Yi Han, Tansu Alpcan, Jeffrey Chan, Christopher Leckie, Benjamin I. P. Rubinstein, "A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning", IEEE Transactions on information Forensics and Security, volume.11,no.3,pp.556–570, 2015.

[25] Deepika Saxena, Ishu Gupta, Jitendra Kumar, Ashutosh Kumar Singh, Xiaoqing, "A Secure and Multi-objective Virtual Machine Placement Framework for Cloud Data Centre", IEEE Systems Journal, volume.16, no.2, pp. 3163 – 3174,2021.

[26] Sakshi Chhabra,Ashutosh Kumar Singh, "A secure vm allocation scheme to preserve against co-resident threat", International Journal of Web Engineering and Technology, volume. 15, no. 1, pp. 96–115, 2020.

[27] Vu Duc Long,Ta Nguyen Binh Duong,"Group Instance: Flexible Co-Location Resistant Virtual Machine Placement in IaaS Clouds",IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 64-69,2020. DOI: 10.1109/WETICE49692.2020.00021.

[28] Nguyen Binh Duong, Neha Pimpalkar, Handling Co-Resident Attacks: A Case for Cost-Efficient Dedicated Resource Provisioning. IEEE 11th International Conference on Cloud Computing (CLOUD), pp.849-852,2018, DOI: 10.1109/CLOUD.2018.00119.

[29] David Siegmund, "The Sequential Probability Ratio Test" Sequential Analysis, Springer Series in Statistics book series (SSS), Chapter.2, pp.8-33, 1985.

[30] T. Padmavathy,R. Anitha, "An efficient virtual machine allocation using single stage weapon target assignment model in cloud software-defined network environment", International Journal of communication systems, volume 35,no. 6, 2022.

Authors

Nelli Chandrakala completed M.Tech from JNTUniversity,Anantapur in 2008 .The research Interests Includes Cloud computing, computer networks and Information Security. Presently she is a research scholar in department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation'Guntur, AP, India.

Dr. Vamsidhar Enireddy completed M.Tech from Andhra University in 2008 and Ph.D. from JNTU Kakinada in 2017.The research Interests Includes Image processing, Machine Learning, DataMining models and Neural Networks. Presently he is working as a Professor in department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation'Guntur, AP, India.

RESEARCH ARTICLE

How to cite this article:

Nelli Chandrakala, Vamsidhar Enireddy, “Multi-Criteria Optimization Based VM Placement Strategy to Mitigate Co-Location Risks in Data Centers”, International Journal of Computer Networks and Applications (IJCNA), 9(5), PP: 510-521, 2022, DOI: 10.22247/ijcna/2022/215912.