A HEURISTIC MODEL FOR SECURING VIRTUAL MACHINE MIGRATION DURING ATTACK TRACES IN CLOUD ENVIRONMENT

Nelli Chandrakala[1]

[1]Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram, AP, India.
[1]Email: kala5136@gmail.com

Vamsidhar Enireddy[2]

[2]Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram, AP, India
[2]Email: vamsidhar@kluniversity.in

Abstract

Various organizations and companies rely on the virtualized environment for running the applications. These sorts of applications require security policies and rigorous protection mechanisms. The significant challenge towards virtualized system availability is software aging which leads to the system collapsing or encounters some failure. Upgrading the software is the only way to handle the aging issues where the researchers recommend the use of VM migration to diminish the downtime. However, there is a gap in security implications during the VM migration-based scheduling. Here, a novel security evaluation method is proposed to assist the model available for the virtualized system. The target is to predict the scheduling without any threat intervention to reach the expected level (availability and security risk). Here, a novel aggregation of heuristic optimizer (A-HO) for system configuration in VM migration is proposed to measure the security threats like DoS, DDoS, Man-in-the-middle. The outcomes offer insight towards the information regarding the security risk and availability when applying the migration scheduling with the aggregation process.

Keywords- Virtualized environmentt, VM migration, migration schedulingg, aggregation process, security risks, heuristic optimizer.

1.Introduction

Recently, the research provides the security information in cloud computing needs extra enhancements that have been studied broadly in the last years [1]. Asymmetric benefits of attackers are one of the most complicated problems in cloud computing security. The robust defenses are established that cost greater than the cost to conduct the attacks in cyber security [2]. However, when the system is protected by the defenders from complete attack vendors, the attackers exploit the single system vulnerability. The benefit of asymmetric is reduced by Moving Target Defense (MTD) [3] that uses the reconfiguration of dynamic circumstance to focus on the thwarting and defending attacks [4]. The important concept of shifting the surface of attacks continuously enhances the difficulties on the reconnaissance circumstance or works on the attacks in a dynamic manner [5]. VM migration is the common strategy for the MTD in the cloud. The VMs are moved for preventing them is the standard technique from co-resident VMs attacks or the available physical hosts [6].

Moreover, the evaluation techniques are required for the security benefits to be quantified and affect the availability during the adoption of various scheduling of VM migration like Moving Target Defence that is opposed to the insider attacks, namely ., MTD timing problem. An algorithm is proposed by Chauhan et al. [7] to select the timing of MTD properly to reduce the assigned costs. The insights are given by the work on the process of evaluating the various MTD timing techniques. The group of MTD techniques are proposed by Sidhu et al. [8] are opposed to the attacks of

Multi-Armed Bandit (MAB) policy. A similar threat model is considered in work. Instead of MAB models, the multi-stage attack that is the attacker needs to reconnoitre the circumstance first before the attack is launched and is considered. A Markov model is proposed by Abdel et al. [9] to evaluate the performance on the deployment of MTD in the virtualized circumstance. The insights are provided by the work. They are (a) the process of modelling the issue of MTD and (b) validation via simulation. The straightforward techniques are followed to apply the general VM migration scheduling as Moving Target Defence is the particular third-party software implementation of MTD is not required [10]. However, the proposed system provides the analysis that focuses on the comparison of various environmental configurations that are various system architectures and VM migration scheduling and advantages are shown. The disadvantages concerned the probability and availability of successful attacks [11]. Further, the analysis provides the tolerance level metric in the proposed system. The tolerance levels are used for supporting the selection of VMs, like the selection of candidates for the deployment of MTD on the predicted runtime related to the attack success tolerated levels probabilities.

The stochastic Reward Net (SRN) model is presented in a proposed model for determining the insider attack success probability with the moving target defense related to the scheduling of VM migration in the Infrastructure-as-a-Service (IaaS) of cloud computing. An important aim is to determine the security and availability of MTD deployment in various situations [12]. Various system architectures are comprised by these situations that are the group of possible physical machine pools and various scheduling policies of VM migration. The moving target defence is considered to focus on the VM attacker's movement among the available physical machine pools [13]. A unique hypervisor is contained in every physical machine pool. The hypervisor is considered as the objective of the insider attacks [14]. Henceforth, every time that the VM is moved, the hypervisor variant is reconnoitered by the attacker prior to proceeding.

The below questions are helped this study [15]. They are:

- RQ1: when utilizing various system architectures, what is the minimization probability of attack success?

- RQ2: Because of various scheduling of VM migration, what are the availability and attack success probability impacts?

- RQ3: Considering various VM migration scheduling and architectures, what time is needed for the system to attain the particular probability of attack success of the tolerance level?

Two case studies are evaluated to address these questions [15]. The reduction of attack success probability is concentrated first during the system architecture is enlarged to four physical machine pools from one physical machine pool. A reduction of attack success probability is examined in the second case study that varies the scheduling of VM migration. The policies are considered with 24 hours, 12 hours, 6 hours, 1 hour, and 30 minutes among the VM migrations. The trade off between security and availability are highlighted in the results. Considering an instance that applies the 30 minutes policy to the system having four physical machine pools, then the probability of attack success at 24 hours is below 1%. The probability is 23% when the 12 hours policies are applied with similar conditions.

This proposed system examines the process of various environmental configurations that creates the impacts on the availability and security levels of an Infrastructure-as-a-Service cloud having the scheduling of VM migration like MTD that is opposed to the insider attack. The scheduling of VM migration is applied already in many contexts like load balancing, sustainability, and software rejuvenation. Moreover, the VM migration achieves 8 seconds at 24 hours for the 12 hours policy and for the 30 minutes policy, 3 minutes are considered, and then the system has downtime. This proposed system contributes to the interest of the system managers who need to develop the scheduling policies of multi-objective VM migration.

2. Related Works

Various computing requirements are given as services in the IT industry. Various advantages are available by using the methodology that is available from the cloud service providers like the on-demand, flexible computing infrastructures, and access to large-scale. Moreover, the dependability on cloud computing is increased, and that is essential to realize the potential. In cloud computing, because of the importance and sensitivity of the stored information, one of the most crucial topics in the cloud circumstance is data security as the cloud service providers' trust. In cloud computing, the malevolent insiders are the risk factors and the cloud services are failed that attains great attraction from the users of the cloud [16]. The development opportunity is provided by cloud computing, and it provides the circumstance for the multi-source information service (MSIS) new service pattern. The nature part of the relationship between cloud computing and MSIS [7] and clouds are associated with the problems. The distributed and shared computing services and resources are offered by the cloud computing that exists to the various websites and service providers. A special focus is needed to pertain the cloud security as one of the essential considerations. Trust management [18] is a vital component of cloud computing. The important problems to pertain the data security in the circumstance of cloud computing, such as the location of data, transmission of data, availability of data, and security of data, are explained. The security problems in cloud computing are explored by Akter et al. [19], and the important research difficulties are highlighted, which has the malevolent insiders, performance and availability, disruptions of service, and outside attacks.

Garg et al. [20] discussed the data security and privacy protection problems in cloud computing. There are three levels that are defined by the security architecture. They are (i) platform security, (ii) software security, and (iii) infrastructure security. In cloud computing, the problems related to data privacy protection in the data lifecycle have the use, transfer, storage, share, destruction, and archival. The security problems in the cloud computing systems are mentioned by the cloud computing issues that are specific to model the management of security that depends on the security standards, and the security problems have pertained to the standards of security. Because of the security and privacy problems of service in cloud computing, the important difficulties are highlighted in the large-scale acceptance. This is recommended based on the described situations that are to reduce the sensitive information if the data is processed and provides the privacy to the user on the cloud needs to assure. The security problem becomes an overwhelming issue to cloud service providers as the number of dependents is shooting up on the cloud service. These problems need to mention first to make use of the advantages of the cloud to a great extremity. Important security problems are mentioned in cloud computing, and a few countermeasures are insisted and implemented in [21]. The security problems are classified into six parts that are presented. The cloud server needs to monitor malevolent insiders tasks, the confidentiality of data, hijacking the service, and problems because of the multi-tenancy. The users are enabled to control across data, and the data loss is prevented are the privacy problems and are discussed when the replication of data occurs. Different security problems such as confidentiality, privacy, trust, availability, and integrity are addressed. Trustworthiness is the applicable word as the information is sourced from the security limits of the owner in the cloud computing environment.

“Wrapper attack” is discussed by [22], who wrapped the attacker with few malevolent codes in the signature of XML, and the signature is injected into the XML codes that are necessary for resource sharing in cloud computing. Cybercrime is the tempting target in cloud computing. Mechanisms used in Amazon and Google are the prominent providers for defending that are opposed to this kind of attack. There are numerous heterogeneous entities comprised in the cloud computing environment. The securities of these circumstances depend on the security promised by the weakest entity. Various delivery models have different security problems [23] in the cloud that threaten the cloud's users. The different problems are mentioned in the proposed system in the software as a Service (SaaS) model, such as confidentiality of data, security of web application, breaches of data, vulnerability in virtualization, backup, availability, management of identity, the process of sign-on. Particularly, in cloud computing, information management has security operations that are a complicated process. The complicated environment is created by the layers of cloud service and the multi-tenancy virtual architecture for developing and managing the security of information related to the compliance program and the incident management. The protection of cloud services over the existing and new attacks is the goal that complies with the regulatory requirements and the security policies. The better-managed services are provided by the suggested technique for the customers who need to outsource information security operations for attaining transparent, reliable, and effective privacy and cloud security [24]. The velocity is increased, guaranteed by cloud computing having the different application types for deployment, lower costs, and increased innovation. The demand deployment, virtualization, internet delivery of services and open-source software is incorporated by cloud computing. Due to the changes in cloud computing, everything is new from another perspective: inventing, developing, deploying, scaling, updating, maintaining, and paying for the infrastructure and application. A flexible and efficient dynamic security approach is needed to make sure the users' data correctness in the cloud due to the advantages of cloud computing. The key aspect is the quality of service, and henceforth the large data security of the cloud and the performance is needed [25].

3. System Model

A group of architectures are considered in the proposed system that ranges from one physical machine pool with various physical machine pools. There are some characteristics in the considered architecture. They are (i) the unique hypervisor variant is in every physical machine pool with the hypervisor is the target of insider attacks of the attacker, (ii) the VMs migration is possible among the physical machine pool, and (iii) At least one physical machine is possible in every physical machine pool for receiving the migrations is shown in Fig 1.

3.1 Threat model

The insider attack that needs to be performed by the attacker is the goal to target the hypervisor that is the middleware among the physical host and VMs. The attacker needs to be monitored or compromised the co-resident VMs when the hypervisor control is assumed. The resignation is not done by the attacker till the success of the attack is assumed in the proposed system. There are two phases in the insider attack. They are (a) reconnaissance that expresses during the attacker needs to be identified the hosts' variant of hypervisor, and (b) attack expresses when the malevolent actions are performed by the attacker that is opposed to the host hypervisor, The attacker chooses the try and error technique in the phase of the attack. Successively, when the time provided on a similar physical host is longer, the chance of attack success is greater. Moreover, can be continued the technique of try and error, and the attempts which are failed are ignored; that is, the knowledge is accumulated by the attacker when the attacker reconnoiters the hypervisor of the host.

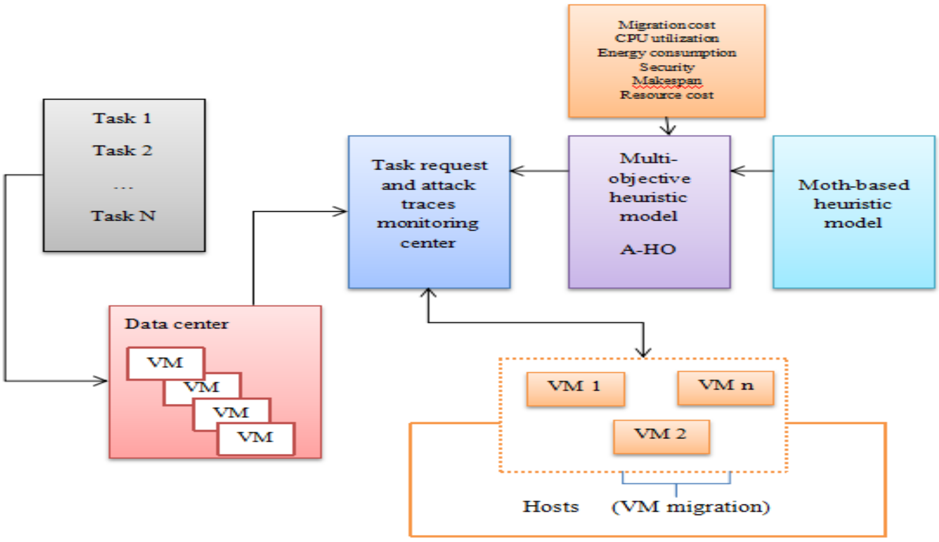

Fig. 1. VM migration-based system model

3.2 Cloud platform

Consider a cloud platform where the resource pools are composed of servers S_i and set of resources is $S_i \; where \; i = 1,2,\ldots,n$. VM are accepted on the server at every node and specified as $S_i = VM_{i,1},\ldots,VM_{i,k}$. Here, $VM_{i,k}$ specifies the VM over the server S_i, every server contains enormous resources like memory, CPU and networks. The determination of host for VM allocation is essential. The client needs demand for services and it has to fulfil QoS requirements. It needs some prerequisites and it needs to undertake some task to VM over the cloud. The set of VM helps in task planning as specified by VM resource allocation and task requirements. Every task is characterized with certain parameters like CPU utilization, security, energy consumption, make span, resource and migration cost are depicted as the key terms for effectual VM migration. It is explained with the optimization problem.

3.3 Fulfilling multi-objective constraints

The foremost objective relies on minimization and it is expressed as in Eq. (1):

$$Objective = \min\{U_{CPU}, Energy, security, makespan, migration\ cost, resource\ cost\} \quad (1)$$

1) CPU utilization is the time consumed by CPU to execute certain tasks. When there is a rise for resource demand in cloud, VM are mapped towards the available server. It is considered to fulfil the CPU requirement with the objective of eliminating delay. It is expressed as in Eq. (2):

$$U_{CPU}\ (task\ allocation) = \sum Count_{CPU}\ (T_1 + \cdots + T_n\} \quad (2)$$

2) Energy consumption: It shows direct relationship with physical machine (PM) utilization. It is depicted as the total amount of energy consumed for certain time and it is expressed as in Eq. (3):

$$Energy\ consumption = 0.1\log(Count_{CPU}) + Energy_i + 0.1 \tag{3}$$

3) Security establishment: The VM migration has to be performed in a secure manner without any intervention of threats like MITM, DoS attacks or both. The VM security is evaluated based on the difference among the task security and physical machine. The evaluation is done based on risk probability.

4) Makespan measure: It is a hypothesis in scheduling the completion time of certain task. It is measured as the maximal wall time to the overall task blocks. It is expressed as in Eq. (4):

$$Makespan\ (tasks) = \max\left(\sum_{i=1}^{N} W_{time}\right) \tag{4}$$

5) Migration cost: It is measured based on scheduling algorithm. It is recurrence of relocation execution. It is connected with prize capacity. It is known as the sum of cost incurred during migration from one to another task by VM and it is expressed as in Eq. (5):

$$Migration\ cost = \sum_{T_i=1}^{n} migration\ cost\ (T_{i=1,2,\dots,n}) \tag{5}$$

6) Resource cost: The relocation process relies on 1) memory content and 2) memory update over every VM; 3) data transfer ability and 4) remaining burden among the server and the source. It is depicted as the sum of resource cost incurred by certain resources to perform related tasks. It is expressed as in Eq. (6):

$$Resource\ cost\ (tasks) = \sum resoruce_{cost}\ (T_1 + \cdots + T_n) \tag{6}$$

3.4 Aggregation of heuristic optimizer (A-HO)

Here, a novel approach is proposed with moth heuristic optimizer to measure the VM migration process and security. The traversing process needs to ensure the moth movement. The following are the steps to fulfil the requirements:

1) The overall moth population and flames are $moth_m$ and $flame_w$ which needs to initialized. The flame count is set as $count_{flames}$ and q specifies the iteration count. The random variable movement is $rand1$ and $rand2$. Then, compute the fitness function.

2) The moth position and flames are updated based on the conventional method. The traversing mechanism for position update is provided and expressed based on Eq. (7):

$$Moth_m = S(moth_m, flame_w) \tag{7}$$

3) The searching agent-based position update is expressed as in Eq. (8):

$$S(moth_m, flame_w) = R_m . e^{ht} . \cos(2\pi t) = Flame_w \tag{8}$$

Here, R_m specifies the logarithmic spiral shape of w^{th} flame and it is expressed as in Eq. (9):

$$R_m = |moth_m - flame_w| \tag{9}$$

Here, R is random number (constant) and t value ranges from [-1, 1].

4) Over successive iteration, the flame counts are evaluated with Eq. (10):

$$Count_{flame} = round\left(N - q * \frac{N-1}{T}\right) \tag{10}$$

Here, N and T specifies the maximal flame count and maximal iterations count. If rand value is higher than 0.5, then the distance among the flames are evaluated and it is expressed as in Eq. (11) & Eq. (12):

$$distance = best_{position}\ (flame) - moth_{position} \tag{11}$$

$$moth_{position} = distance + best\ position\ (flame) \tag{12}$$

5) When $q > count_{flames}$, then $rand < 0.5$. The moth and flame position is updated and it is described as in Eq. (10) to Eq. (13). Similarly, when rand > 0.5, then the position update of searching agent is provided with some novel method and the distance computation among the flame from moth using Eq. (13) to Eq. (14) is expressed as in Eq. (13) & Eq. (14):

$$distance = best_{position}\ (flame) - sort\ (population) \tag{13}$$

$$moth_{position} = distance + best\ position\ (flame) \tag{14}$$

The algorithm for the anticipated model is given below:

Algorithm 1:

```
Initialize overall population with moth and flames;
Initialize rand1, rand2 and $count_{fitness}$;
Compute fitness value as in Eq. (1);
for $(q_{max} > q)$
If termination criteria ≠ fulfilled;
if $\left(q \leq count_{flame}\right)$
if $(rand < 0.5)$
Transverse mechanism performs flame and moth position updation as in Eq. (7);
Perform spiral position update with searching agent as in Eq. (8);
Flame count is given in Eq. (10);
else
evaluate the distance among the moth and flame;
elseif
else if $(q > count_{flame})$
if $(rand < 0.5)$
perform traversing with moth and flame based position update in Eq. (7);
perform spiral position update with search agent using Eq. (8) to Eq. (10);
end if
end if
end
terminate the process
```

The computation of VM migration is to fulfil security and other multi-objective constraints synthetically. The data is related with PM and acquired from online available Kaggle data set for cloud. With the available data set, the related data is connected with VM are executed. The parameters connected with the execution process are provided in Table 1.

PM count	Original data
Total tasks	Synthetic data
Wall time	
PM cost	
Security	
CPU count	

Table 1. Parameter setup

The VM data set is created with the assistance of PM data set. Also, it encompasses certain PM parameters. Consider, the task is related with the PM as $T_i = 1,2,3,4$. The task block size of task 1, 2, 3, and 4 and it is set as 5, 10, 15 and 12 respectively. The task attained from the user is assigned to PM and the tasks and the corresponding schedules are related with separate VM. Here, 12 PM is used and every PM is intended to have 10 VM. Therefore, there is totally 120 VM to execute certain tasks.

1) Security – The security of PM ranges from 1 to 4 randomly. It is determined as an essential factor and the evaluation of VM is done based on the task and PM security. The value of PM and VM is set between 1 to 4. When the security value of PM is set as 1, then the task value is set as 1. Finally, the VM security is 0. Therefore, the model needs to

fulfil the security requirements based on risk mechanism. When the task count is set as 6, then the security values bounded among 1 to 4. The task-based security value is 1 and it is termed as highly secured and the lesser security task is taken based on higher security value, i.e., 4.

2) Wall time – It is depicted as the measure of time during the active process with certain task. The difference among these two depends on run-time factors, i.e. system waiting and programmed delays. The PM is pre-determined with wall time. It is evaluated with normal random function. It is expressed as in Eq. (15):

$$W_{time} = normal\ rand\ (\mu, \delta) \tag{15}$$

3) VM cost- It is measured with the normal random function. Here, δ is set as 0.1 and μ represents PM cost as depicted in Eq. (16):

$$VM_{cost} = normal\ rand\ (\mu, \delta) \tag{16}$$

4) Migration cost- It is evaluated from $M * M$ matrix and the rows and columns are considered for measuring the PM cost. Here, the matrix is equal to rows and columns, i.e. (1,1), (2,2) and provides diminishes migration cost and higher migration cost.

5) Energy consumption: The VM energy consumption is evaluated with normal random function. It is expressed as in Eq. (17):

$$Energy\ consumption = normal\ rand\ (\mu, \delta) \tag{17}$$

Here, the overall energy consumed by the PM is set as 60 watts and the mean is normal random function. The SD is produced with random number $\pm 5\%$ when the task in block is 1 and accomplished with CPU utilization, PM and VM. The CPU utilization is added and the over utilization count is evaluated for all tasks with the summation process.

4. Results and Discussion

The anticipated VM migration against malicious threats is provided for establishing the model's efficiency and the simulation is done in MATLAB 2020a environment and the performance of the anticipated model is analyzed with various metrics like energy consumption, cost, response time, migration cost and security. The proposed model is compared with various existing heuristic methods like ABC, ACO, SA, WO, GWO and LO. The evaluation outcomes may vary from one VM to other. VM may varies for all PM.

VM	ABC	ACO	SA	WO	GWO	LO	Proposed moth
10	935	1300	1250	1200	4700	5600	880
20	1700	1500	1200	1800	3200	5070	1200
30	1600	1100	1250	1250	3300	2214	965
40	1600	1600	1500	1600	1800	3120	1130
50	980	1311	1200	2250	2400	5818	1300

Table 2. CPU Utilization

VM	ABC	ACO	SA	WO	GWO	LO	Proposed moth
10	2400	2530	2564	2589	2400	2555	2456
20	2400	2580	2456	2590	2500	2564	2324
30	2450	2560	2589	2548	2560	2456	2500
40	2500	2525	2600	2589	2525	2896	2600
50	2520	2531	2564	2561	2635	2654	2361

Table 3. Energy consumption

VM	ABC	ACO	SA	WO	GWO	LO	Proposed moth
10	285	370	290	305	525	310	280
20	330	333	375	320	390	390	350
30	360	310	350	330	600	460	280
40	420	280	375	365	540	370	300
50	320	385	350	390	610	330	375

Table 4. Makes pan comparison

VM	ABC	ACO	SA	WO	GWO	LO	Proposed moth
10	290	260	250	290	230	280	88
20	270	250	255	265	250	260	190
30	220	250	242	245	70	230	220
40	230	270	295	290	245	280	154
50	220	210	300	250	75	280	145

Table 5. Migration cost

VM	ABC	ACO	SA	WO	GWO	LO	Proposed moth
10	0.088	0.068	0.118	0.122	0.500	0.281	0.224
20	0.092	0.082	0.078	0.136	0.188	0.188	0.272
30	0.165	0.102	0.068	0.161	0.604	0.155	0.204
40	0.133	0.192	0.092	0.171	0.365	0.210	0.258
50	0.088	0.222	0.108	0.128	0.584	0.315	0.323

Table 6. Security comparison

Table VII. Resource costVM	ABC	ACO	SA	WO	GWO	LO	Proposed moth
10	52.2	31.7	52.2	42.03	56.9	63.2	21.2
20	30.6	34.1	30.6	48.10	43.7	50.2	27.8
30	29.8	29.4	29.8	46.40	55.2	24.4	24.3
40	28.9	49.3	28.9	46.9	34.6	48.6	23.9
50	34.5	45.5	34.2	32.25	41.7	67.3	25.4

Table. 7 Resource cost

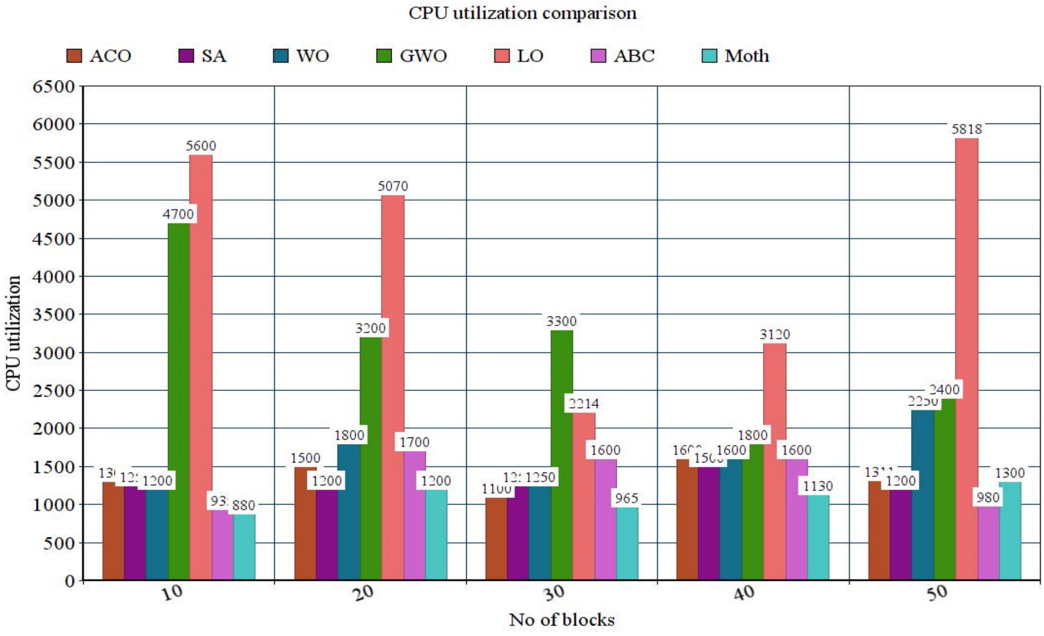

Fig. 2. CPU utilization comparison

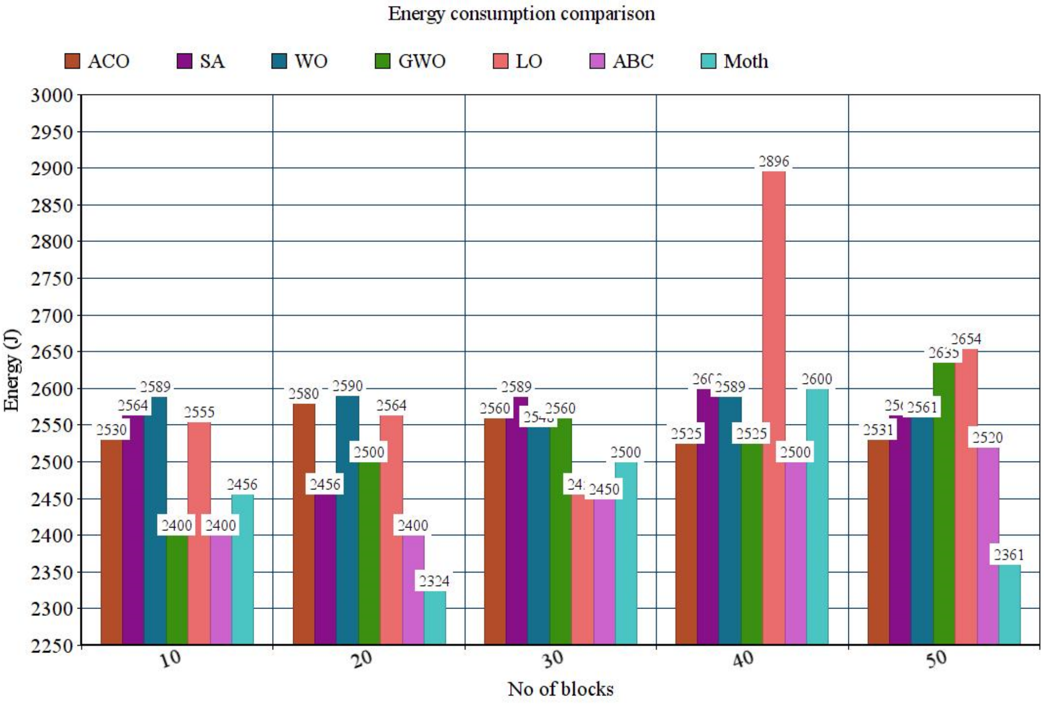

Fig .3. Energy consumption comparison

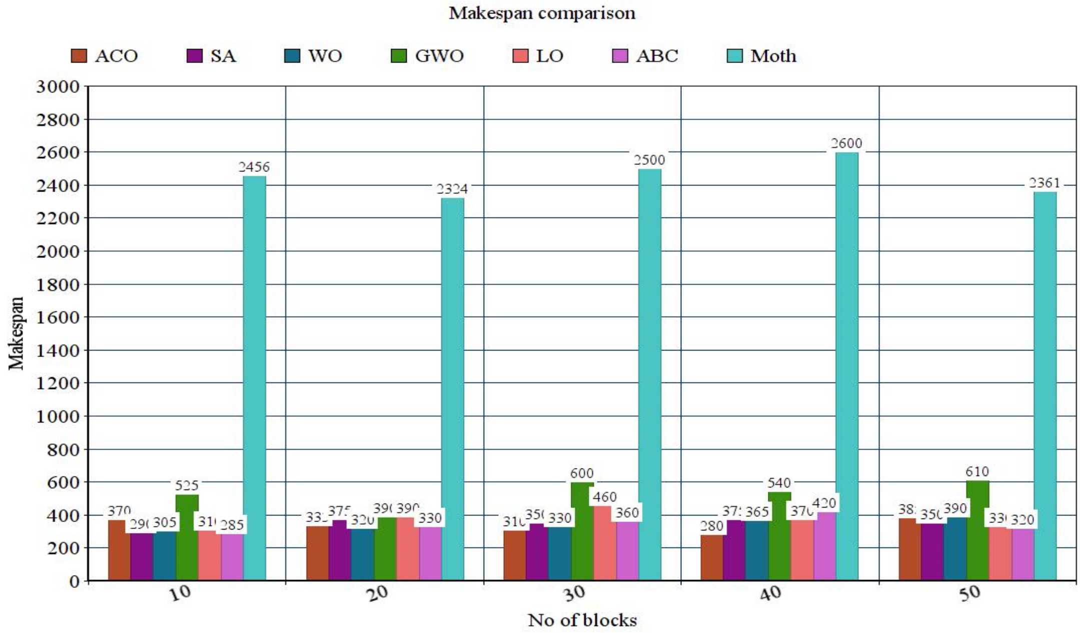

Fig.4.Makespan comparison

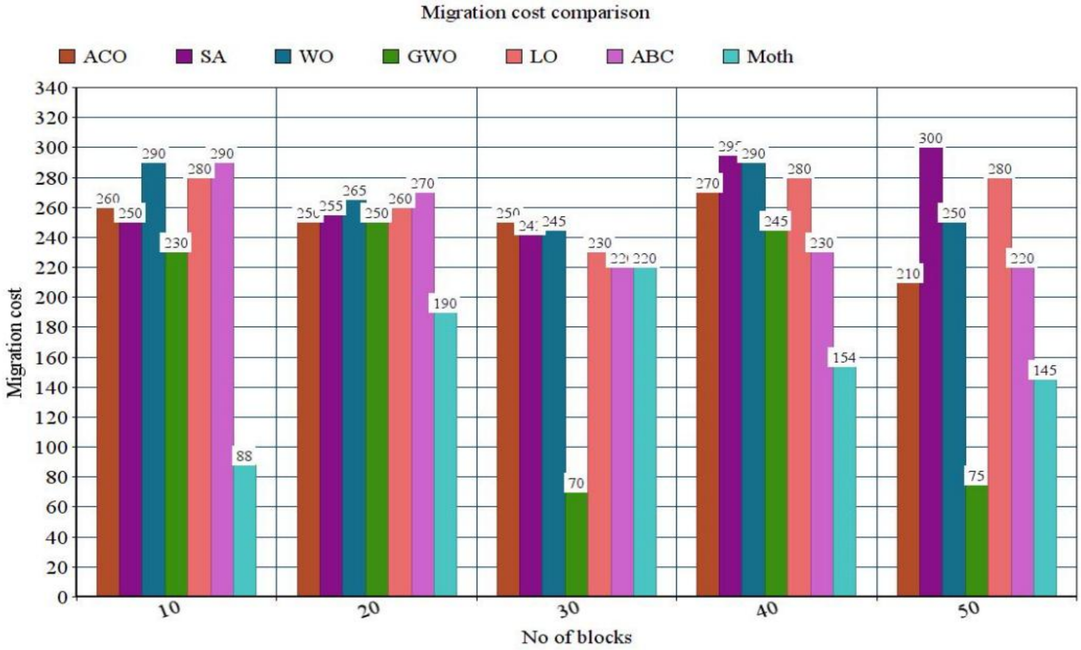

Fig. 5. Migration cost comparison

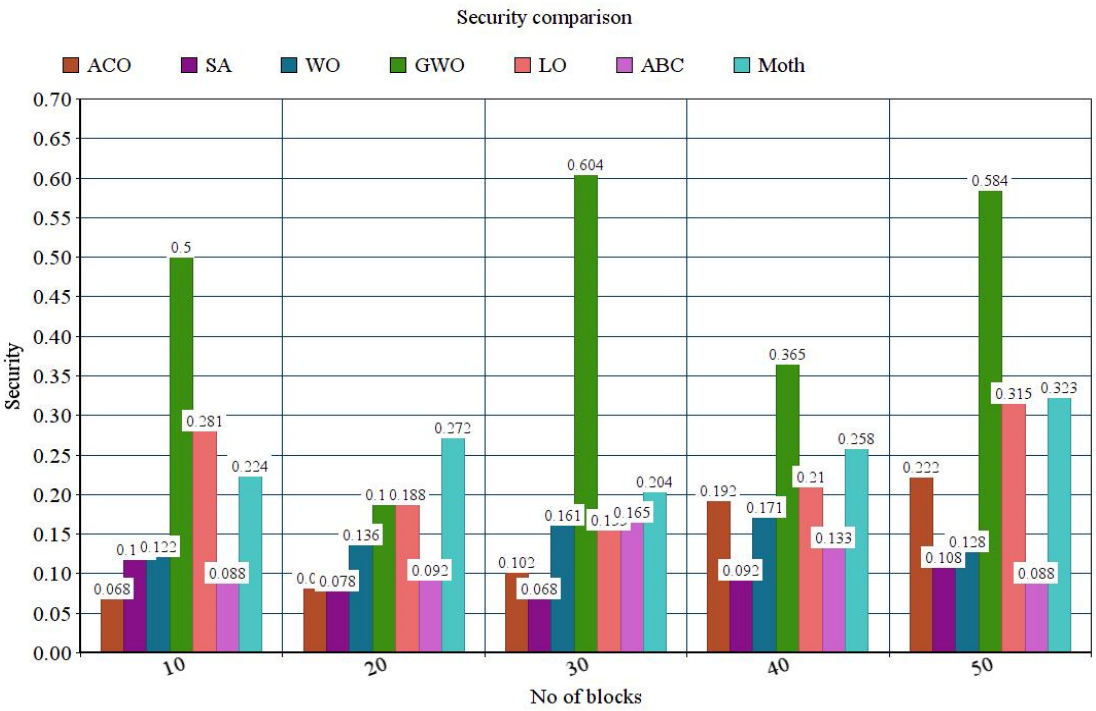

Fig. 6. Security comparison

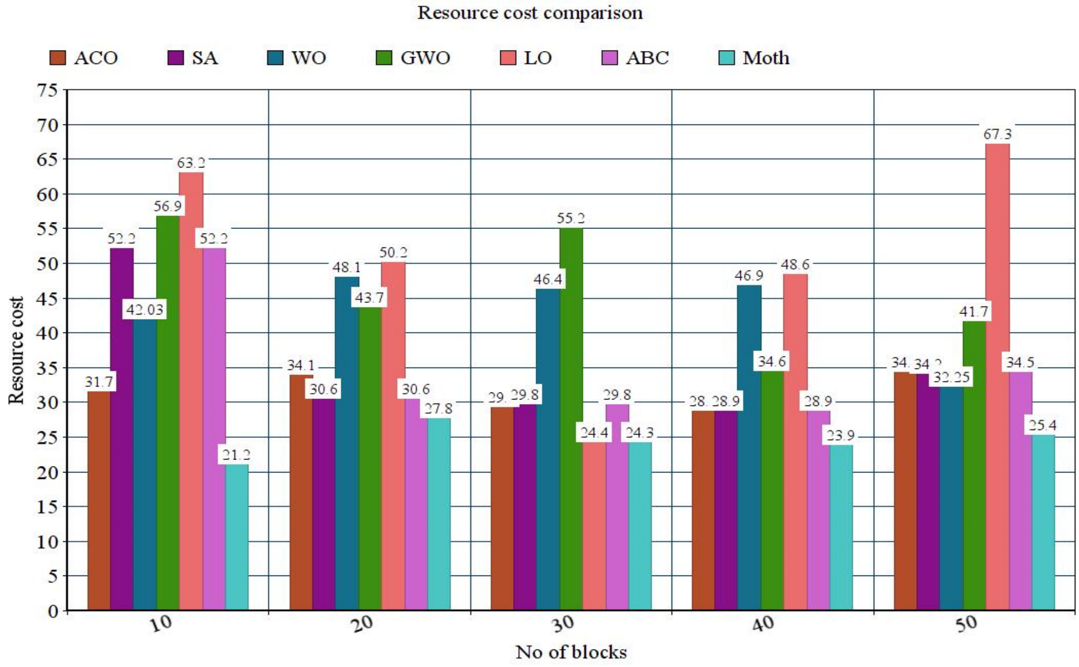

Fig. 7. Resource cost comparison

Table 2 depicts the comparison of CPU utilization. Here, 10 to 50 VM blocks are considered. However, the comparison is made among 50th VM block. The CPU utilization of the anticipated heuristic model is 1300 which is optimal compared to other approaches like ABC, ACO, SA, WO, GWO and LO models. The CPU utilization of ABC is 980, ACO is 1311, SA is 1200, WO is 2250, GWO is 2400 and LO is 5818 and is shown in Fig 2. Table 3 depicts the comparison of energy consumption among the provided heuristic model. The energy consumed by the anticipated model is 2361 Joule which is lesser than other optimization models. The ABC consumes 2520 J, ACO is 2531 J, SA is 2564 J, WO is 2561 J, GWO is 2635 J and LO is 2654 J respectively and is shown in Fig .3. Table 4 depicts the comparison of make span comparison. The anticipated model is nominal with 375, while ABC is 320, ACO is 385, SA is 350, WO is 390, GWO is 610 and LO is 330 and is shown in Fig 4. Table 5 depicts the migration cost of the anticipated model with other approaches. The moth model shows a migration cost of 145, ABC is 220, ACO is 210, SA is 300, WO is 250, GWO is 75 and LO is 280 and shown in Fig 5. Table 6 depicts the security-based comparison of the anticipated model with other approaches and is shown in Fig.6. The security established by moth is 0.323%, ABC is 0.088%, ACO is 0.222%, SA is 0.108%, WO is 0.128%, GWO is 0.584% and LO is 0.315%. Table 7 depicts the comparison of the resource cost of the anticipated model with other approaches and is shown in Fig.7. The moth model shows a resource cost of 25.4, ABC is 34.5, ACO is 45.5, SA is 34.2, WO is 32.25, GWO is 41.7 and LO is 67.3. Based on all these observations, it is proven that the anticipated model works well in fulfilling the multi-objective constraints compared to other models.

5. Conclusion

This work intends to model an efficient approach for handling VM migration even in case of malicious activities like DoS, MITM and combination of both. However, this issue turns into a multi-objective constraint. Various investigators intend to handle this issue; but fails in any of one aspect. The anticipated moth heuristic model addresses all the research constraints and provides superior solution compared to other approaches. Some performance metrics like security, response time, energy consumption, migration cost is analysed and compared with other approaches like ABC, ACO, SA, GWO and LO. The anticipated moth heuristic model gives superior outcomes compared to other approaches. In the future, the hybridized model is adopted to enhance the prediction outcomes. Here, a aggregation of heuristic optimizer (A-HO) for system configuration in VM migration is used to measure the security threats like DoS, DDoS, Man-in-the-middle. The outcomes offer insight towards the information regarding the security risk and availability when applying the migration scheduling with the aggregation process.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] Sukhpal Singh Gill, Rajkumar Buyya. (2018): A taxonomy and future directions for sustainable cloud computing: 360-degree view. ACM Computing Surveys 51(5), pp.1–33.

[2] Buyya R, Srirama SN, Casale G, Calheiros R, Simmhan Y, Varghese B, Gelenbe E, Javadi B, Vaquero LM, Netto MA, et al. (2018): A manifesto for future generation cloud computing: Research directions for the next decade. ACM Computing Surveys 51(5), pp.1–38.

[3] Liaqat M, Chang V, Gani A, Hamid SHA, Toseef M, Shoaib U, Ali RL. (2017): Federated cloud resource management: Review and discussion. Journal of Network and Computer Applications 77(1), pp.87–105.

[4] Kogias DG, Xevgenis MG, Patrikakis CZ. (2016): Cloud federation and the evolution of cloud computing. Computer 49(11), pp.96–99.

[5] Kun Ma, Antoine Bagula, Olasupo O. Ajayi. (2019): Quality of service (QoS) modelling in federated cloud computing. arXiv:1911.03051 [cs.DC].

[6] Eisa M, Younas M, Basu K, Awan I. (2020): Modelling and simulation of QoS-aware service selection in cloud computing. Simulation Modelling Practice and Theory 103,102108.

[7] Chauhan SS, Pilli ES, Joshi R, Singh G (2018): UPB: User preference-based brokering for service ranking and selection in the federated cloud. IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). pp 1–6.

[8] Sidhu J, Singh S Jagpreet Sidhu. (2017): Improved topics method-based trust evaluation framework for determining the trustworthiness of cloud service providers. Journal of grid computing 15(1):pp.81–105.

[9] Abdel-Basset, M.; Mohamed, M.; Chang V, (2018), NMCDA: a framework for evaluating cloud computing services. Future Generation Computer Systems. 86, pp.12–29.

[10] M. Chandni; N. P. Sowmiya; S. Mohana; M. K. Sandhya (2017): Establishing trust despite attacks in cloud computing: a survey. International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 712–716.

[11] Georgopoulos, Z.; Lambrinoudakis, C.(2016): Literature review of trust models for cloud computing. 15th International Symposium on Parallel and Distributed Computing (ISPDC), pp. 208–213.

[12] Mohamed, B.; Youness, K.I.; Mohamed M. (2016): Taking account of trust when adopting cloud computing architecture. 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), pp. 101–106 .

[13] Yefeng, R.; Durresi, A. (2017): A trust management framework for cloud computing platforms. In: IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), pp. 1146–1153.

[14] Abdullah M AL-Faifi.;Atif Alamri.;Mohammad Mehedi Hassan.;Biao Song (2019): A hybrid multi-criteria decision method for cloud service selection from intelligent data. Future Generation Computer Systems. 94, pp.43–57.

[15] Ahmed mansour Manasrah.; Dr.Ammar Almomani.; Tariq Alsmad.(2016): A variable service broker routing policy for data centre selection in cloud analyst. Journal of King Saud University- Computer and Information Sciences. 29(3), pp. 365–377.

[16] Meesariganda, B.R.; Ishizaka, A. (2017): Mapping verbal AHP scale to numerical scale for cloud computing strategy selection. Applied Soft computing. 53, pp.111–118.

[17] Kou, G.; Ergo, D.; Lin, C.; Chen, Y. (2016): Pairwise comparison matrix in multiple criteria decision making. Technological and Economic Development of Economy. 22(5), pp.738–765.

[18] Bertolino, A.; Angelis, G.D.; Gallego, M.; García, B.; Gortázar, F.; Lonetti, F.; Marchetti, E.(2019):A systematic review on cloud testing. ACM Computing Surveys (CSUR), 52 (5), pp.1–42.

[19] Akter, M.; Gani, A.; Rahman, M.O.(2018); Hassan, M.M.; Almgren, A.; Ahmad, S. :Performance Analysis of Personal Cloud Storage Services for Mobile Multimedia Health Record Management. IEEE Access, 6, pp. 52625–52638.

[20] Garg, S.K.; Versteeg, S.; Buyya, R. (2011): SMICloud: A framework for comparing and ranking cloud services. In Proceedings of the 4th IEEE International Conference on Utility and Cloud Computing, Melbourne, VIC, Australia; pp. 210–218.

[21] Vasilios, A.; Darsow, A.; Karastoyanova, D.; Leymann, F.(2014): CloudDSF—The Cloud Decision Support Framework for Application Migration; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany.; pp. 1–16.

[22] Sáez, S.G.; Andrikopoulos, V.; Bitsaki, M.; Leymann, F.; Van Hoorn, A.(2018): Utility-based decision making for migrating cloud-based applications. ACM Transactions on Internet Technology, 18 (2),pp. 1–22.

[23] Wenbin Yao.; Liang Lu (2015): A selection algorithm of service providers for optimized data placement in the multi-cloud storage environment," Communications in Computer and Information Science.(CCIS503) Springer, pp. 81–92.

[24] Tricomi, G.;Panarello, A.; Merlino, G.; Longo, F.; Bruno, D.; Puliafito,A.(2017) ''Orchestrated multi-cloud application deployment in OpenStack with TOSCA,'' IEEE International Conference Smart Computing (SMARTCOMP), pp. 1–6.

[25] Jrad, J.;Tao, A. ;Streit, R.; Knapper, ; Flath, C. (2015):A utility-based approach for customized cloud service selection," International Journal of Computer Science and Engineering, 10(1/2), pp. 32-44.

[26] Esposito, C. ;Ficco, M.; Palmieri, F.; Castiglione,A.(2016) :''Smart cloud storage service selection based on fuzzy logic, theory of evidence and game theory,'' IEEE Transactions on Computers, 65(8), pp. 2348–2362.

[27] Thiruselvan Subramanian.; Nickolas Savarimuthu.;(2015): Application based brokering algorithm for optimal resource provisioning in multiple heterogeneous clouds, Vietnam Journal of Computer Science, 3, pp. 57–70.

[28] Dan Lin, Anna Cinzia Squicciarini, Venkata Nagarjuna Dondapati, Smitha Sundareswaran (2019)''A cloud brokerage architecture for efficient cloud service selection,'' IEEE Transactions on Services Computing., 12(1), pp. 144–157.

[29] Elhabbash, A.; Elkhatib,Y.; Blair, GY. ;Lin,Y.; Barker,A. :(2019)''A framework for SLO-driven cloud specification and brokerage, 19th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. (CCGRID), pp. 666–667.

[30] Sabrina De Capitani di Vimercati, ; SaraForesti,; Giovanni Livraga,; Piuri, V. ; Samarati, P. (2019) :A fuzzy-based brokering service for cloud plan selection, IEEE Systems Journal, 13(4), pp. 4101–4109.

Authors Profile

Nelli Chandrakala completed M.Tech from JNT University, 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, Data Mining 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