An Artificial Intelligence (AI) based Energy Efficient and Secured Virtual Machine Allocation Model in Cloud

Nawaf Alhebaishi
Department of Information Systems, Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah, Saudi Arabia
nalhebaishi@kau.edu.sa

2022 3rd International Conference on Computing, Analytics and Networks (ICAN) | 978-1-6654-9944-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICAN56228.2022.10007164

***Abstract*— Ensuring security in cloud systems is one of the most significant tasks for users facing security problems in load balancing. Many conventional works have developed secured load balancing models for allocating Virtual Machines (VMs) in cloud systems. Still, it limits by the problems of high migration overhead, increased processing time, storage complexity, high energy consumption, and lack of security. So, the proposed work objects to implement an energy-efficient and secured Artificial Intelligence (AI) based VM allocation model for cloud load balancing. The novel contribution of this work is to develop an Intelligent Mine Blow Optimization (IBMO) technique to securely allocate the VMs in the cloud. Also, it helps to mitigate the security risks created by the attacks of VMs from multiple users. Moreover, it maintains the workloads among all VMs in the cloud server. The primary advantages of this work are reduced energy consumption, resource consumption, and overhead. During analysis, the performance and results of the proposed IBMO-based VM allocation model are validated and compared using various evaluation indicators.**

Keywords— Cloud Systems, Virtual Machine (VM) allocation, Resource Sharing, Optimization, Artificial Intelligence (AI), and Security.

I. INTRODUCTION

Due to the rapid growth of information technology, cloud systems [1, 2] have recently gained significant attention. Also, it plays a vital role in modern society, and provides enormous applications to the users. However, the traffic rate is exponential increased in the cloud systems due to their increase usage of applications. Hence, it is highly essential to satisfy the requirements of Virtual Machines (VMs), which supports to balance the loads across the cloud systems [3]. In cloud data centers, traffic has grown tremendously due to the quick growth of applications. It is becoming increasingly typical to relocate VMs to other hosts for better load balancing in order to meet the performance needs of VMs. Secure VM allocation has drawn a lot of attention as one of the biggest issues with cloud computing. Because multiple occupants share the same resources, sharing confidential data in the cloud has always been risky for users. Accomplishing a secure load balancing to map virtual machines (VMs) onto secure physical machines that are a security conscious VM for task deployment. According to the recent reports, it is analyzed that a secured VM allocation is still remains one of the major problem need to be addressed in the cloud systems. Typically, the users have an increased risk [4, 5] while sharing the confidential data among various cloud systems, because multiple users can share the same resources. So, there is an increased possibility for the threats or attacks [6], for instance, attackers/malicious users can steal the confidential information of the legitimate parties, when all VMs executed on the same cloud server. This type of attacks [7] can be identified and detected by blocking the VMs before execution. Due to this facet, developing a secured load balancing scheme [8, 9] in cloud is one of the challenging and highly demanding tasks in present times. Generally, the resource allocation mechanisms [10-13] in cloud are categorized into the following types:

1. Mapping of workloads
2. Mapping of VMs

In the conventional works, the different types of optimization mechanisms [14-16] are developed for securely allocating the VMs in the cloud systems. However, it limits with the key problems of increased migration overhead, more time consumption, complexity in processing, and high energy consumption [17, 18]. Therefore, the proposed work intends to develop an energy efficient and secured Artificial Intelligence (AI) based VM allocation model for cloud load balancing. By using a computationally efficient optimization algorithm, the process of resource allocation is properly performed in the proposed work, which helps to significantly reduce the migration overhead, processing time, storage complexity, and energy consumption. Since, the optimization based scheduling is also strengthens the security of the cloud system. The major research objectives of this work are as follows:

- To develop an energy efficient and secured scheduling algorithm for allocating VMs in the cloud data center.
- To strengthen the security of overall scheduling
- system against the attacks of VMs from multiple users.
- To effectively minimize the resource and cost consumption of VM allocation model, an Intelligent Mine Blow Optimization (IBMO) technique is deployed.

- To simplify the process of scheduling with increased efficiency, and security.
- To validate the performance of the proposed optimization based scheduling mechanism, various evaluation indicators such as Service Level Agreement (SLA) violations, energy consumption, and execution time have been considered.

The other portions of this paper are structured into the following sections: Section II reviews the conventional AI mechanisms used for scheduling the VMs in the cloud systems. It also investigates the pros and cons of each technique based on its features and characteristics. Section III presents the description about the proposed optimization based resource scheduling mechanism used for VM allocation in the cloud server. Section IV presents the evaluation results of conventional and proposed optimization based scheduling techniques using various parameters. Finally, the overall paper is concluded with its future work in Section V.

II. Related Works

This section reviews the conventional AI based optimal scheduling mechanisms for allocating VMs in the cloud systems. Also, it discusses about the advantages and disadvantages of each technique according to its operating functions and key features.

Ousmane et al. [19] implemented a game theoretic approach for properly allocating the VMs in cloud systems. The main contribution of this work was to obtain the new solution for identifying the VM escape attack for ensuring the cloud security. Moreover, it objects to improve the system efficiency, utility functions and minimize the attack cost. Mahipal et al. [20] developed a new VM allocation policy to solve the interdependency problems in the cloud environment. It mainly objects to determine the attackers' success probability based on the security parameters of efficiency and coverage. Also, the secured potential host was identified before allocating the VMs in the cloud environment. However, it follows some complex computational operations, which affects the performance of entire system. Huang et al. [21] deployed an advanced optimization based allocation scheme for scheduling the VMs and PMs in the cloud data center according to the user specifications. The purpose of this work was to minimize the energy consumption, improve the CPU utilization rate, and reliability by using the optimization technique. Here, two different algorithms such as user request allocation, and migration have been utilized for ensuring the better data transmission rate. The primary advantage of this work was, it efficiently reduced the energy utilization rate by optimally allocating the resources in cloud. Zhou et al. [22] implemented an adaptive energy aware VM allocation mechanism for solving the problems of load fluctuation and energy efficiency. Here, the different types of energy aware scheduling mechanisms used in the cloud-IoT systems were investigated in terms of energy, threshold, type of allocation, and workload.

Zhang et al. [23] deployed an energy efficient evolutionary approach for properly allocating the VMs with reduced time consumption. The purpose of this work was to implement the service reservation process for maximizing the energy efficiency of VM allocation in cloud data centers. Yet, this work limits with the major problems of inefficient computations, reduced convergence rate, and complexity. Gao et al. [24] implemented an auction based allocation mechanism for scheduling the VMs across the edge cloud systems. Typically, the proper VM allocation in edge cloud systems was one of the most challenging and important problem need to be addressed in recent times. The primary advantages of this work were increased efficiency, truthfulness, and minimal time consumption. However, it follows some complex mathematical operations to scheduling the resources across the VMs, which affects the performance of entire cloud systems. Samriya et al. [25] introduced a multi-objective Emperor Penguin Optimization (EPO) technique for allocating VMs in the heterogeneous cloud systems with minimal energy consumption. The purpose of this paper was to optimally allocate the resources among the VMs with reduced time and energy consumption. Here, the placement optimizer was utilized to optimize the energy, Service Level Agreement (SLA), and resource constraints. Moreover, the performance of this work was validated in terms of computational complexity, space complexity, and time complexity. The key benefits of this work were optimized memory consumption, energy consumption, and better convergence rate.

Gill et al. [26] implemented a new conceptual model for allocating the VMs in cloud systems with improved Quality of Service (QoS). The main purpose of this work was to incorporate IoT, blockchain, and AI technologies for solving the complex problems in the next generation systems. Mohiddin et al. [27] introduced a Workload Aware Virtual Machine Consolidation Method (WAVMCM) for optimally scheduling the workloads in the cloud systems. The key contribution of this work was to develop an efficient VM management model with reduced resource utilization and energy consumption. Shalu et al. [28] employed an Artificial Neural Network (ANN) mechanism for allocating VMs in the cloud environment. It also implemented an Enhanced Modified Best Fit Decreasing (E-MBFD) algorithm for solving the VM placement problem with efficient resource utilization. For validating the performance of this technique, the propagation error, Mean Squared Error (MSE), and power consumption. Razaque et al. [29] developed an Energy Efficient and Secure Hybrid (EESH) algorithm for strengthening the security of cloud fog systems. In addition, the Malicious Data Detection (MDD) algorithm was also utilized with the blockchain methodology for enabling secured data transmission. Navabi et al. [30] designed a new mechanism, named as, TRACTOR for increasing the security level of cloud systems. Here, an ABC based optimization technique was also used to optimize the network traffic by properly managing VMs. Table I presents the comparative analysis of conventional scheduling mechanisms used for VM allocation with its benefits and demerits. According to this review, it is analyzed that the conventional works are mainly focused on developing an optimization techniques for resource allocation in cloud. Still, it limits with the challenges of increased migration overhead, high resource consumption, time requirement, and complex scheduling operations. Therefore, the proposed work intends to deploy a new optimization based scheduling technique for an efficient workload balancing in the cloud systems.

TABLE I. COMPARATIVE ANALYSIS AMONG THE CONVENTIONAL SCHEDULING MECHANISMS

References	Technique	Problems Addressed	Pros & Cons
[31]	PSO based scheduling	Allocation of VMs in the cloud server.	1. Reduced energy consumption. 2. Inefficient scheduling and increased processing time.
[32]	Dynamic server allocation linear program	It objects to dynamically allocate the VMs.	1. Energy efficient 2. Minimal server demand 3. Migration overhead
[33]	Gossip protocol	It intends to allocate the computing and network resources.	1. Simple to implement 2. It requires increased resources for execution
[6]	Fast slow down algorithm	It allocates the VMs by predicting the load based on optimal solution.	1. Energy saving 2. Not highly efficient
[34]	Artificial Bee Colony (ABC) optimization	It intends to identify the optimal solution for resource allocation.	1. Energy efficiency 2. High overhead 3. Inefficient workload balancing

III. PROPOSED METHODOLOGY

This section presents the detailed description about the proposed secured VM allocation strategy in the cloud environment. The original contribution of this work was to develop an advanced optimization based AI model for securely allocating the VMs in cloud with increased energy efficiency and reduced resource consumption. For this purpose, an Intelligence Mine Blow Optimization (IMBO) technique is deployed, which provides the optimal solution for allocating the VMs in cloud server. The architecture and working flow model of the proposed AI based VM allocation system is shown in Fig. 1 and Fig. 2 respectively, which includes the major stages of VM allocation and security model. It maps VMs onto secure PMs that a security conscious VM for task deployment by achieving a secure load balancing method. The goal of this study is to reduce the likelihood of attacks between various users. It certainly decreases information leakage during load balancing and enhances cloud infrastructure security. When allocating VMs, it checks for safe and unsafe conditions and which offers superior flexibility and quality controls. As a result, changing the requirements of the client is quite simple. Finally, allocations might be adjusted up or down in according to the requirements. The key contributions of this work are as follows:

- To solve the security risks created by the attacks of VMs from multiple users.
- To minimize the overall energy and resource consumption in the scheduling system.
- To equally maintain the workloads among the VMs in the cloud server.

A. Secured VM Allocation

This work developed an Intelligent Mine Blow Optimization (IBMO) mechanism for properly scheduling the resources across the VMs. Here, the problem of secured VM allocation in cloud is efficiently solved with the optimal solution of IBMO. Let consider, the cloud receives N number

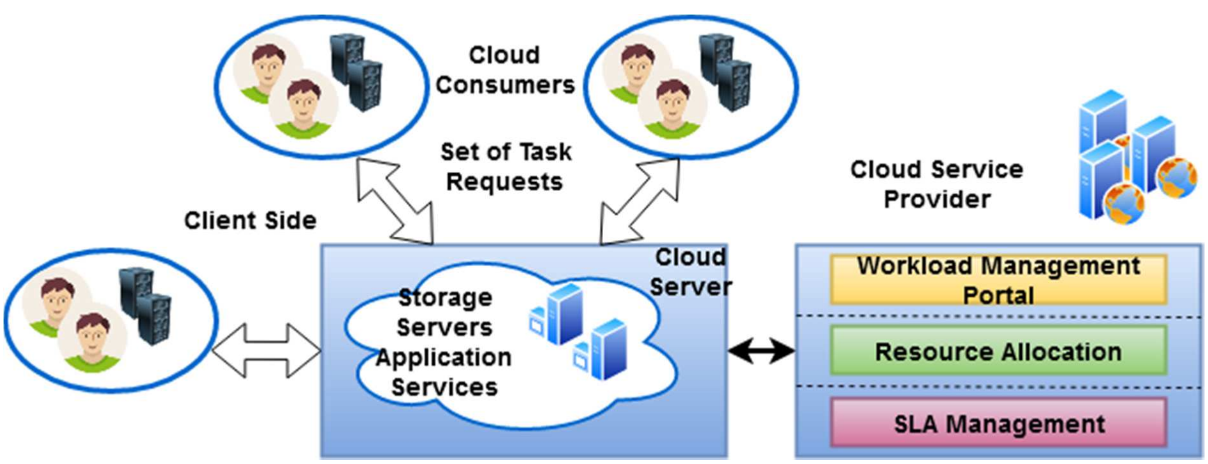

Fig. 1. Architecture model of secured VM allocation in cloud

performances. In this framework, the workload is efficiently balanced with the proper allocation of resources, SLA management, and overall workload scheduling in the cloud calculates the client's dependability based on previous system, of requests N_{VM} from N number of users N_U, where each VM describes the workload as the static value. Then, the cloud assigns the VMs to the available number of physical servers N_S, which is in the range of $[N_S^{min}, N_S^{max}]$. Based on the workload

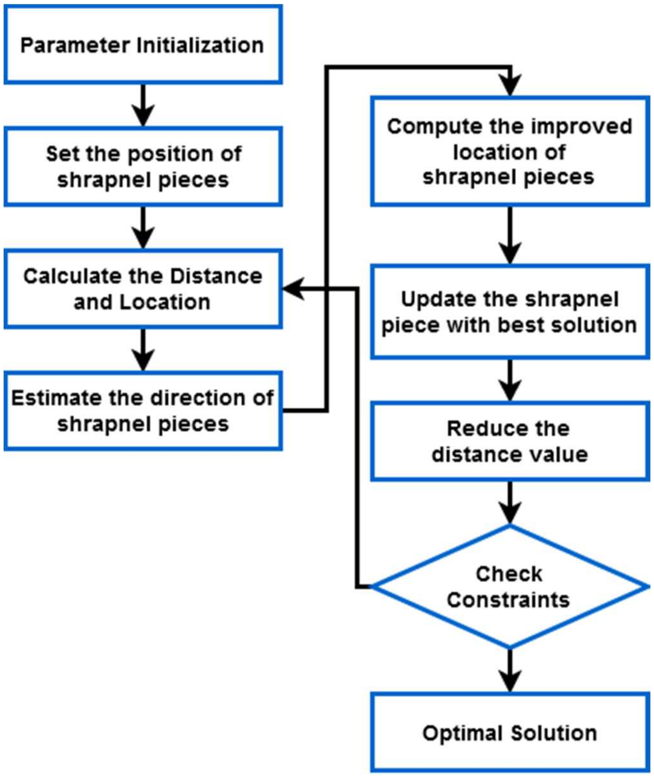

Fig. 2. Working flow of IMBO

requirements, the VMs are squeezed into various servers, which helps all the servers to reach the full capacity. Consequently, the maximum number of servers are achieved, when the VM is allocated to a different physical servers. Typically, the cloud has the ability to calculate the proportion of malicious users, but it does not predict that which user is malicious. When it identifies the malicious user, it is considered that all VMs from the user are malicious. Based on these assumption, an energy efficient and secured VM allocation mechanism is developed with the help of IBMO. The key contribution of using this technique to resolve the security problems with better power efficiency and reduced energy consumption. This goal is achieved based on the following model:

$$CV = \omega_1 \times S_R + \omega_2 \times F_E(U) + \omega_3 \times W_{PS} \quad (1)$$

Where, $\omega_1, \omega_2, \omega_3$ are the weight values, CV indicates the cost value, S_R denotes the security risk, F_E is the energy consumption, and W_{PS} is the workload inequality among various physical servers. Based on this model, the cost value is optimized as follows:

$$S_R = M_U \times \frac{\sum_{i=1}^{N_S}(N_{CL}^i - 1)}{N_S \times (N_U - 1)} \quad (2)$$

Where, M_U is the malicious users, N_S denotes the actual number of servers, N_U is the actual number of users, and N_{CL}^i defines the number of co-located users. Here, the energy rate is estimated according to the CPU utilization rate as shown in below:

$$F_E(U) = \frac{E_h - E_l}{A_h - A_l} U - \frac{E_h A_l - E_l A_h}{A_h - A_l} \quad (3)$$

Where, $E_{h,} E_l$ are the higher and lower energy, and A_h, A_l are the higher and lower utilization rate. Consequently, the normalized energy cost E_{nor} is estimated as follows:

$$E_{nor} = \frac{\sum_{i=1}^{N_S} |CE_i - CE_{best}|}{CE_{best} \times N_S} \quad (4)$$

Where, CE_i is the energy cost of i[th] server, and CE_{best} denotes an efficient energy cost. Finally, the workload inequality cost is normalized by using the following model:

$$W_{PS} = \frac{1}{N_S} \sqrt[2]{\sum_{i=1}^{N_S} (WL_i - \overline{WL})^2} \quad (5)$$

Where, WL is the workload of VM, and $\overline{WL}$ indicates the average workload. Based on this process, the security risk against the attacks of VMs from multiple users is efficiently avoided.

B. Intelligent Mine Blow Optimization (IBMO) mechanism

In the proposed system, the primary reason of using an IBMO technique is to efficiently allocate the VMs in the cloud system with reduced energy consumption and increased security. Typically, the IBMO is a kind of meta-heuristic optimization model mainly developed for solving the multi-objective and complex problems with the desired solutions. Here, the purpose of implementing this technique is to obtain the best optimal solution with reduced number of iterations and cost consumption. The key benefits of using this approach are global searching capability, reaches the optimal solution with reduced number of iterations, and better exploration. This optimization technique is mainly used to ensure the secured VM allocation in the cloud systems. In this model, the maximum energy, when compared to the other approaches. From the number of iterations and the search space dimensionality are initialized based on the upper bound and lower bound values by using the following models:

$$P = \{P_b\}, b = 1,2,3, \dots, S_d \quad (6)$$

$$P_0 = lb + K_D * (ub - lb) \quad (7)$$

Where, S_d indicates the dimension of search space, P_0 defines the initial variable, K_D is the features, ub and lb are the upper and lower bound values respectively. After that, the distance and location of the shrapnel fragments are identified, if the exploration components is satisfied. Then, the direction of shrapnel is estimated as illustrated below:

$$D_{n+1}^m = \frac{G_{n+1}^m - G_n^m}{P_{n+1}^m - P_n^m} \quad (8)$$

Where, D_{n+1}^m denotes the direction, G_{n+1}^m and G_n^m are the objective functions at *n* and $(n+1)^{th}$ iterations. Moreover, the fragments are created based on the updated placements by using the following model:

$$P_{n+1}^m = P_{s(n+1)}^m + \exp\left(-\sqrt{\frac{D_{n+1}^m}{a_{n+1}^m}}\right) P_n^m \quad (9)$$

Based on this function, the constraints are verified to determine that whether the shrapnel is created or not. Consequently, the best shrapnel fragments are considered as the best temporary solution. Then, its positions are updated to find out the best optimal temporal solution. The distance and location of the best shrapnel bits are defined based on the following models:

$$P_{s(n+1)}^m = d_n^m * rand * \cos(\varphi) \quad (10)$$

$$a_{n+1}^{m} = \sqrt{(P_{n+1}^{m} - P_{n}^{m})^2 + (G_{n+1}^{m} - G_{n}^{m})^2} \quad (11)$$

Furthermore, the shrapnel's distance is optimally minimized as shown in below:

$$a_{n}^{m} = \frac{a_{n-1}^{m}}{\exp(q/\rho)} \quad (12)$$

Where, ρ *and* q indicates the reduction constants and iteration number index correspondingly. At last, the convergence criterion is validated to identify the optimal fitness value, which is used to optimally allocate the resources in the cloud systems.

IV. Results and Discussion

This section validates the performance and results of the proposed AI based secured VM allocation mechanism by using various evaluation indicators. Also, the obtained results of the proposed methodology is compared with some of the recent-state-of-the-art approaches for proving the betterment of the proposed scheduling system. Table II and Fig. 3 validates the energy consumption rate of conventional [25], and proposed optimization based VM allocation mechanisms. In cloud systems, energy consumption is estimated by the total amount of energy required by the PMs in the cloud systems. For ensuring the better performance of the scheduling system, the energy consumption should be minimized. Based on the obtained results, it is analyzed that the proposed optimization based scheduling mechanism consumes the reduced amount of graph and table, it can be seen that as the number of VMs increases, the energy usage of the data center also increased. The estimated results indicate that the proposed approach helps to efficiently minimize the energy consumption even with the increase of number of VMs.

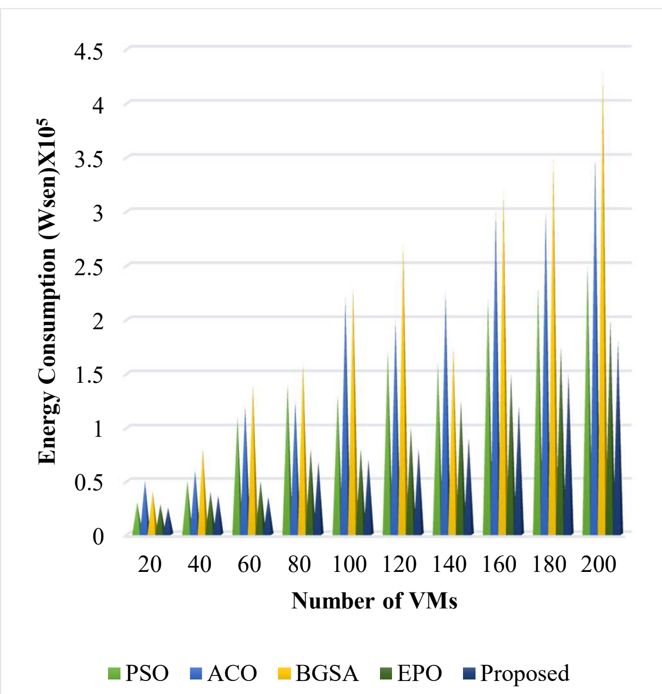

Fig. 3. Energy consumption

TABLE II. Energy analysis

VM placed	PSO	ACO	BGSA	EPO	Proposed
20	0.3	0.5	0.4	0.28	0.25
40	0.5	0.6	0.8	0.4	0.36
60	1.1	1.2	1.4	0.5	0.35
80	1.4	1.25	1.6	0.8	0.68
100	1.3	2.2	2.3	0.8	0.7
120	1.7	2	2.7	1	0.8
140	1.6	2.25	1.75	1.25	0.9
160	2.2	3	3.2	1.5	1.2
180	2.3	3	3.5	1.75	1.5
200	2.5	3.5	4.3	2	1.8

Table III and Fig. 4 depicts the SLA violations of the conventional and proposed optimization based scheduling techniques. Typically, the SLA violations can be created due to the over usage of PMs. Moreover, the SLA violations should be minimum for ensuring the better system performance. Also, it helps to minimize the resource wastage by properly utilizing the CPU for operations. Based on the obtained results, it is evident that the proposed IBMO based scheduling technique efficiently minimizes the SLA violations, when compared to the other techniques. Similarly, the execution time is also estimated for the conventional and proposed optimization based scheduling techniques with respect to varying number of VMs as shown in Table IV and Fig. 5. Typically, the execution time is defined as the total amount of time required to accomplish the scheduling process. Also, the minimal execution time assures the improved system performance. From the evaluation, it is analyzed that the proposed IBMO technique requires reduced time consumption, when compared to the other techniques. Specifically, the lower execution time helps to minimize the overall system complexity. Due to its larger computational complexity compared to the other three algorithms, the BGSA algorithm takes longer time to execute. The PSO algorithm results in greater energy usage than using the ACO method because its execution time is faster. Additionally, we found that the proposed algorithm's execution time is faster than that of the BGSA, EPO, ACO, and PSO approaches, and its rate of convergence is very high. The shorter execution time of the suggested technique lowers the system's overall complexity.

TABLE III. Comparative analysis based on Service Level Agreement (SLA)

No of VMs	BGSA	ACO	PSO	EPO	Proposed
40	9	11	12	7	6.5
80	9.2	10	8.2	9	8
120	10.2	10.1	10	9.3	9
160	8.8	8	9.6	8.2	7.8
200	10	10	10	8.5	8.2

TABLE IV. Execution time analysis

No of VMs	BGSA	ACO	PSO	EPO	Proposed
40	0	10	8	0	0
80	60	50	10	10	8
120	110	120	50	20	18
160	250	220	150	50	45
200	500	400	250	80	70

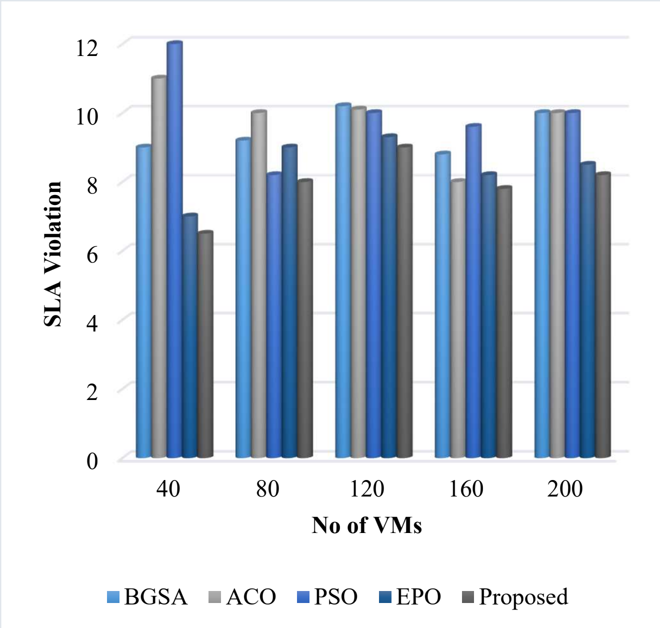

Fig. 4. SLA violations

Table V and Fig. 6 compares the energy consumption of various and proposed VM scheduling techniques with respect to the number of VMs. This analysis also show that the proposed technique requires reduced energy consumption, when compared to the other techniques due to the optimization based proper scheduling. Moreover, the number of PMs used in the cloud data center is validated for both conventional and proposed scheduling techniques as shown in Table VI and Fig 7. From the obtained results, it is evident that the proposed IBMO based VM scheduling technique requires the reduced number of PMs for task execution, which shows the overall improved system performance.

Table V. Comparative analysis based on energy consumption

Number of VMs	SSUR	FFD	MBFD	Proposed
100	29.8	29.2	28.4	26.5
500	107.1	163.9	130	104.9
1000	308.9	417.8	392.9	304.8
5000	2894.5	3215.9	3046.2	2893.5

TABLE VI. COMPARATIVE ANALYSIS BASED ON NUMBER OF PHYSICAL MACHINES USED

Number of VMs	SSUR	FFD	MBFD	Proposed
100	10.2	32.8	18.2	9.5
500	22.2	43.7	25.3	20.4
1000	88.4	96.6	90.6	85.2
5000	196.2	202	217.4	194.3

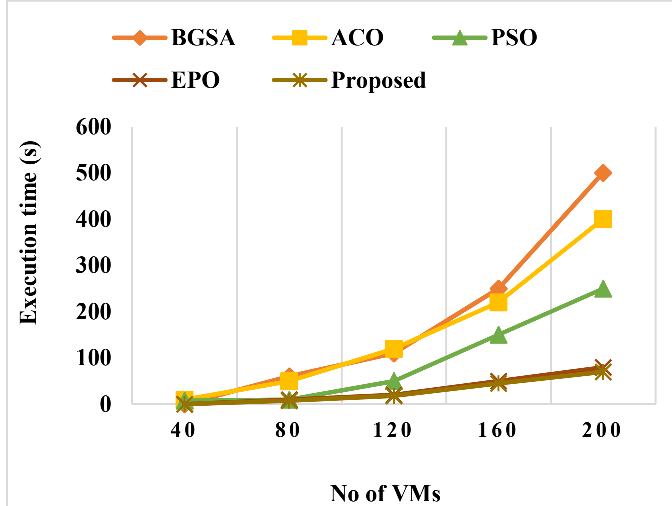

Fig. 5. Execution time

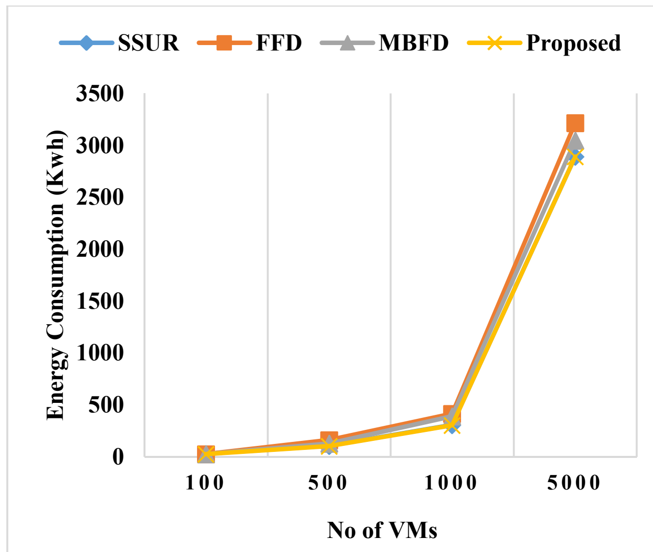

Fig. 6. Energy consumption Vs No of VMs

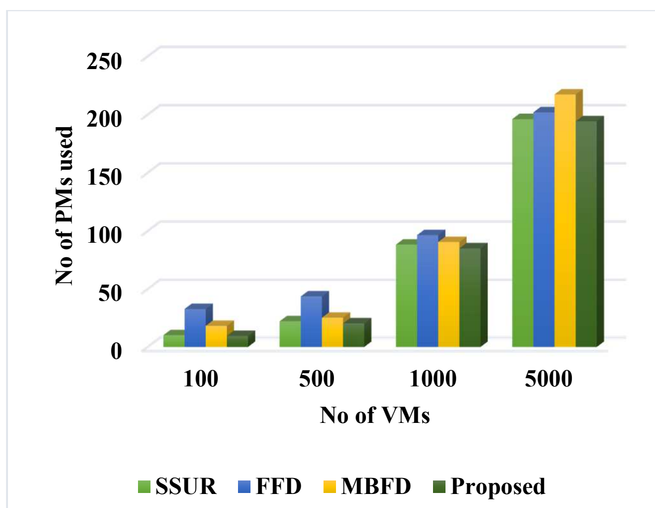

Fig. 7. No of VMs Vs No of PMs used

V. CONCLUSION

This paper presents a new IBMO based scheduling framework for securely allocating VMs in the cloud systems. The main purpose of this work is to develop an AI based energy efficient and secured VM allocation mechanism with reduced computational complexity. By using this approach, the security risks created by the attacks of VMs are efficiently solved, and it equally maintains the workloads among all VMs. Also, it helps to optimize the overall energy and resource consumption of cloud load balancing systems. The primary advantages of using the proposed IBMO technique are global searching capability, reaches the optimal solution with reduced number of iterations, and better exploration. During performance analysis, the results of the proposed optimization based scheduling mechanism is validated in terms of energy consumption, SOA violations, number of PMs used, and execution time. Also, the obtained results are compared with the recent state-of-the-art models for proving the efficiency of the proposed energy efficient and secured VM allocation model. According to the estimated results, it is analyzed that the proposed approach outperforms the other techniques with better performance results. Finally, our suggested approach is superior to others because it saves on average 60% of energy and decreases SLA violations by an average of 50%. Consequently, this approach promotes green computing by reducing the energy use of cloud data centers.

In future, this work can be extended by implementing an advanced security methodology for attack prevention and detection in cloud systems.

REFERENCES

[1] P. Zhang, M. Zhou, and X. Wang, "An intelligent optimization method for optimal virtual machine allocation in cloud data centers," IEEE Transactions on Automation Science and Engineering, vol. 17, pp. 1725-1735, 2020.

[2] M. Soltanshahi, R. Asemi, and N. Shafiei, "Energy-aware virtual machines allocation by krill herd algorithm in cloud data centers," Heliyon, vol. 5, p. e02066, 2019.

[3] X. Ruan, H. Chen, Y. Tian, and S. Yin, "Virtual machine allocation and migration based on performance-to-power ratio in energy-efficient clouds," Future Generation Computer Systems, vol. 100, pp. 380-394, 2019.

[4] A. Akbari, A. Khonsari, and S. M. Ghoreyshi, "Thermal-aware virtual machine allocation for heterogeneous cloud data centers," Energies, vol. 13, p. 2880, 2020.

[5] M. J. Usman, A. S. Ismail, H. Chizari, G. Abdul-Salaam, A. M. Usman, A. Y. Gital, et al., "Energy-efficient virtual machine allocation technique using flower pollination algorithm in cloud datacenter: a panacea to green computing," Journal of Bionic Engineering, vol. 16, pp. 354-366, 2019.

[6] P. S. Rawat, P. Dimri, and G. P. Saroha, "Virtual machine allocation to the task using an optimization method in cloud computing environment," International Journal of Information Technology, vol. 12, pp. 485-493, 2020.

[7] P. Xu, G. He, Z. Li, and Z. Zhang, "An efficient load balancing algorithm for virtual machine allocation based on ant colony optimization," International Journal of Distributed Sensor Networks, vol. 14, p. 1550147718793799, 2018.

[8] Manikandan Thirumalaisamy, Shajahan Basheer, et al., “Interaction of Secure Cloud Network and Crowd Computing for Smart City Data Obfuscation”, in Sensors, MDPI, 2022.

[9] Muralidharan C,Mohamed Sirajudeen Y,Shitharth S,Nawaf Alhebaishi,Rayan H. Mosli,Hassan Haes Alhelou,‘Three-phase service level agreements and trust management model for monitoring and managing the services by trusted cloud broker, IET Commun. pp. 1-12, 2022.

[10] G.Bhageerath Chakravorthy, R.Aditya Vardhan , K. Karthik Shetty, K.Mahesh et al., ‘Handling Tactful Data In Cloud Using Pkg Encryption Technique’ 4th smart city symposium, pp. 338-343, 2021

[11] R. Shaw, E. Howley, and E. Barrett, "Applying reinforcement learning towards automating energy efficient virtual machine consolidation in cloud data centers," Information Systems, vol. 107, p. 101722, 2022.

[12] Rajanikanth Aluvalu, V.Uma Maheswari, Krishna Keerthi Chennam et al.,‘Data Security in Cloud Computing Using Abe-Based Access Control’, Architectural Wireless Networks Solutions and Security Issues, Lecture notes in network and systems, Springer, pp. 47-62, 2021.

[13] Krishna Keerthi Chennam, Rajanikanth Aluvalu and S.Shitharth,‘ An Authentication Model with High Security for Cloud Database’, Architectural Wireless Networks Solutions and Security Issues, Lecture notes in network and systems, Springer, pp. 13-26, 2021.

[14] S. Parida, B. Pati, S. C. Nayak, and C. R. Panigrahi, "Offer based auction mechanism for virtual machine allocation in cloud environment," in Advanced Computing and Intelligent Engineering, ed: Springer, pp. 339-351, 2020.

[15] B. Han and R. Zhang, "Virtual Machine Allocation Strategy Based on Statistical Machine Learning," Mathematical Problems in Engineering, 2022.

[16] D. Kesavaraja and A. Shenbagavalli, "QoE enhancement in cloud virtual machine allocation using Eagle strategy of hybrid krill herd optimization," Journal of Parallel and Distributed Computing, vol. 118, pp. 267-279, 2018.

[17] S. Basu, G. Kannayaram, S. Ramasubbareddy, and C. Venkatasubbaiah, "Improved genetic algorithm for monitoring of virtual machines in cloud environment," in Smart Intelligent Computing and Applications, ed: Springer, pp. 319-326, 2019.

[18] B. Thirumaleshwari Devi, S.Shitharth, ‘An Appraisal over Intrusion Detection systems in cloud computing security attacks’, 2nd International Conference on Innovative Mechanisms for Industry applications, IEEE Explore, ICIMIA -2020, pp. 122.

[19] S. B. Ousmane, B. C. S. Mbacke, and N. Ibrahima, "A game theoretic approach for virtual machine allocation security in cloud computing," in Proceedings of the 2Nd International Conference on Networking, Information Systems & Security, pp. 1-6, 2019.

[20] S. Mahipal and V. C. Sharmila, "Virtual machine security problems and countermeasures for improving quality of service in cloud computing," in 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS), pp. 1319-1324, 2021.

[21] Y. Huang, H. Xu, H. Gao, X. Ma, and W. Hussain, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," IEEE Transactions on Green Communications and Networking, vol. 5, pp. 670-681, 2021.

[22] Z. Zhou, M. Shojafar, M. Alazab, J. Abawajy, and F. Li, "AFED-EF: An energy-efficient VM allocation algorithm for IoT applications in a cloud data center," IEEE Transactions on Green Communications and Networking, vol. 5, pp. 658-669, 2021.

[23] X. Zhang, T. Wu, M. Chen, T. Wei, J. Zhou, S. Hu, et al., "Energy-aware virtual machine allocation for cloud with resource reservation," Journal of Systems and Software, vol. 147, pp. 147-161, 2019.

[24] G. Gao, M. Xiao, J. Wu, H. Huang, S. Wang, and G. Chen, "Auction-based VM allocation for deadline-sensitive tasks in distributed edge cloud," IEEE Transactions on Services Computing, 2019.

[25] J. K. Samriya, S. Chandra Patel, M. Khurana, P. K. Tiwari, and O. Cheikhrouhou, "Intelligent SLA-Aware VM Allocation and Energy Minimization Approach with EPO Algorithm for Cloud Computing Environment," Mathematical Problems in Engineering, vol. 2021, p. 9949995, 2021/05/30 2021.

[26] S. S. Gill, S. Tuli, M. Xu, I. Singh, K. V. Singh, D. Lindsay, et al., "Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges," Internet of Things, vol. 8, p. 100118, 2019.

[27] I. Mohiuddin and A. Almogren, "Workload aware VM consolidation method in edge/cloud computing for IoT applications," Journal of Parallel and Distributed Computing, vol. 123, pp. 204-214, 2019.

[28] Shalu and D. Singh, "Artificial neural network-based virtual machine allocation in cloud computing," Journal of Discrete Mathematical Sciences and Cryptography, vol. 24, pp. 1739-1750, 2021.

[29] A. Razaque, Y. Jararweh, B. Alotaibi, M. Alotaibi, S. Hariri, and M. Almiani, "Energy-efficient and secure mobile fog-based cloud for the Internet of Things," Future Generation Computer Systems, vol. 127, pp. 1-13, 2022.

[30] S. S. Nabavi, S. S. Gill, M. Xu, M. Masdari, and P. Garraghan, "TRACTOR: Traffic-aware and power-efficient virtual machine placement in edge-cloud data centers using artificial bee colony optimization," International Journal of Communication Systems, vol. 35, p. e4747, 2022.

[31] A. Pradhan, S. K. Bisoy, and A. Das, "A survey on PSO based meta-heuristic scheduling mechanism in cloud computing environment," Journal of King Saud University-Computer and Information Sciences, 2021.

[32] N. N. Devi and S. V. Kumar, "SLAV Mitigation and Energy-Efficient VM Allocation Technique Using Improvised Grey Wolf Optimization Algorithm for Cloud Computing," in 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 155-160, 2022.

[33] S. Srivastava, S. Saxena, R. Buyya, M. Kumar, A. Shankar, and B. Bhushan, "CGP: cluster-based gossip protocol for dynamic resource environment in cloud," Simulation Modelling Practice and Theory, vol. 108, p. 102275, 2021.

[34] S. Ouhame, Y. Hadi, and A. Arifullah, "A hybrid grey wolf optimizer and artificial bee colony algorithm used for improvement in resource allocation system for cloud technology," International Journal of Online and Biomedical Engineering (iJOE), 2020.