An Optimal Sanitization Algorithm Based Secure Migration of Virtual Machines in Cloud Datacenters

Nimmol P.John[1] and Bindu V.R

[1]*Research scholar, School of Computer Sciences, Mahatma Gandhi University, Kerala, India*
[2]*Professor, School of Computer Sciences, Mahatma Gandhi University, Kerala, India*
Corresponding Author mail: nimmolpjohn@yahoo.com

Abstract

Cloud is a dominant player in information technology in recent years. In order to meet the increasing demand of computing and storage resources, infrastructure cloud providers are deploying planet scale data centers across the world. These data centers consists stupendous number of servers. These data centers incur very high investments in operational cost, maintenance cost and networking facilities. Because of the huge energy usage, such data centers leave large amount of carbon footprints and thus have adverse effects on the environment. As a result maximum resource utilization and energy consumption are becoming crucial issues to make cloud computing more successful. Intelligent virtual machine migration and consolidation are the primary means to address these issues. However during migration the system integrity and confidentiality of data may be affected. In order to overcome the security issues, this paper proposes a security aware virtual machine migration method. An optimal cryptography algorithm is proposed. This is a combination of sanitization algorithm and orthogonal learning particle swarm optimization (OLPSO) algorithm. This algorithm is used to generate the key and to increase the confidentiality of the migrated data. The performance of the proposed methodology is analyzed and compared in terms of different evaluation metrics.

Keywords: - Security, migration, OLPSO, sanitization, energy consumption, cloud computing, virtual machine.

1. Introduction

Virtual machine migration selects an active virtual machine (VM) and moves it from one physical machine to another. This migration must be transparent to the guest operating system, applications running on the operating system, and to the remote clients of the VM [1]. The migration of VMs can be divided into two different type static migration and live migration. Live migration is the transition of a VM from the source server to the destination server without halting both servers. Keeping the service uninterruptedly is the key requirement for many applications. Live migration is used to achieve load balancing, energy efficiency and easy hardware maintenances [2]. There are several factors that prevent a VM with protected processes running inside from being migrated straightforwardly [3]. VM can be deployed and run on the host machine in a cloud environment. It is easy to migrant VMs between host machines [4]. VM migration is an administrative tool supported by much virtualization software like XEN, VMWARE, KVM, Hyper-V, etc. These provide flexible migration and management of VMs.

Migration of VMs is a useful tool in data centers and cloud environments in which a virtual machine is migrated from one storage location to another for the sake of load balancing or in a scenario where hardware failure is imminent [5]. VMs are utilized to run users applications. With the use of virtualization unutilized resources of physical machines could be additionally utilized by another VM to accelerate the task execution as well as resource utilization [6].So one of the possible approaches for reducing management complexity is to deploy virtualization. In this approach, applications run on virtual servers that are constructed using VMs, and one or more virtual servers are mapped onto each physical server in the system. The migration manager employs provisioning techniques to determine the resource needs of overloaded VMs and uses a greedy algorithm to determine a sequence of moves or swaps to migrate overloaded VMs to under loaded servers [7]. VMs not only provide efficient and secure computing resource containers but also can be migrated smoothly among multiple physical machines. Live migration of virtual machines has been a strong management tool in the multiple VM based environment [8].

Migration at the level of an entire VM means that active memory and execution state is transferred from the source to the destination. Live migration mitigates this problem by allowing administrators to move VMs with little interruption

[9]. The metadata scatter across multiple modules in the VM. They are not part of the migrating VM but describe runtime contexts of protected processes and should be migrated along with the VM. The live migration of VMs imposes even more challenges as the procedure is more complex and may introduce additional security vulnerabilities. As is the nature of VM live migration, VMs are still running while the migration is in the process [10]. VMs allow users to create, copy, save (checkpoint), read and modify, share, migrate and roll back the execution state of machines with all the ease of manipulating a file [11]. Virtualization is an emerging technology that abstracts the physical resources of a computing platform into many separate logical resources or computing environments. Each of the separated virtual computing environments is called a VM [12]. When a VM migrates, filtering rules should be reconfigured at source and destination locations and state related information (e.g. existing connections) stored by state full security appliances and called security context, should be correctly moved to the destination appliances [13]. In this paper we propose a secure virtual machine migration to increase the confidentiality of the data and reduce power consumption. Initially the load of each VM is calculated and depends on load VMS are migrated. In the process of migration the data may get lost. To reduce the security issues data are securely transferred with the help of new proposed optimal cryptography algorithm. Then the performance is evaluated with the help of different metrics. The main contributions of the work are presented here:

- For better security optimal sanitization algorithm is utilized which in turn increases the security of the data.
- For key value optimization OLPSO algorithm is utilized for strongly reducing the information loss.
- The performance is analyzed in terms of encryption time, decryption time, make span and energy consumption.

The rest of the paper is organized as follows. The proposed methodology based research papers are analyzed in section 2 and the proposed methodology is discussed in section 3. The experimental results analyzed in section 4 and conclusion part is presented in section 5.

2. Related Work

A lot of researchers developed secure VM migration for energy consumption in cloud. Among them some of the works are analyzed here. Nawfal *et al*. [14] presented a task scheduling algorithm. That was able to lower the power consumption and reduces the total data center load. The algorithm uses the tasks deadline and VMs load as parameters for scheduling algorithm. The main aim of their work is to reduce the problem of power consumption in data centers and to enhance the load balancing simultaneously. Cloud computing is basically the approach of offering services through their data centers. These data centers need huge amount of power if they are in the peak load or if the tasks are not distributed efficiently in their machines.

Getzi Jeba Leelipushpam Paulraj et al. [15] presented a resource aware VM migration technique. By applying the rule of clustering the servers immediate change in the environment can be identified. By considering the job arrival rate and resource utilization of the destination server the proper target server is selected. Their proposed technique is implemented in cloud platform running analytics on smart agriculture application. The evaluation results show that the proposed method outperforms the state of art techniques in terms of the number of migrations, energy utilization and migration time. It was also demonstrated in real-time that the proposed migration technique does not affect the application functionalities

Getzi Jeba Leelipushpam Paulr *et al* [16] derived a combined forecasting technique to predict the resource requirement of any VM in the cloud. Based on the current and predicted resource utilization live migration is performed by the Combined Forecast Load-Aware technique (CFLA). Experiments were carried out to evaluate the performance of the proposed technique on live VM migration. The outcomes indicate that the proposed approach has minimum number of migrations, energy usage and message overhead when compared with the existing state-of-art techniques.

Clément Dévigne *et al* [17] explained an architecture allowing the execution of fully virtualized multi core operating systems benefiting of hardware cache coherence. The physical isolation is made by the means of address space via the introduction of a light hardware module similar to a memory management unit at the network-on-chip entrance but without the drawback of relying on a page table.

Mostafa Noshy *et al* [18] presented a better understanding of the live migration of VMs and its main approaches. Specifically it focuses on reviewing state-of-the-art optimization techniques devoted for developing live VM migration according to memory migration. It reviews, discusses, analyzes and compares these techniques to realize their optimization and their challenges. The work also highlights the open research issues that necessitate further investigation to optimize the process of live migration for VMs.

Ming Zhao and Renato J. Figueiredo *et al* [19] described about the VM based resource reservation problem that is the reservations of CPU, memory and network resources for individual VM instances, as well as for VM clusters. In particular it considers the scenario where one or several physical servers need to be vacated to start a cluster of VMs for dedicated execution of parallel jobs. VMs provide a primitive for transparently vacating workloads through migration. However the process of migrating several VMs is time consuming and needs to be estimated. To achieve this goal the paper seeks to provide a model that can characterize the VM migration process and predict its performance based on a comprehensive experimental analysis.

Qiang Huang *et al* [20] explained a power consumption evaluation on the effects of live migration of VMs. Results show that the power overhead of migration was much less in the scenario of employing the strategy of consolidation than the regular deployment without using consolidation. The results are based on physical server, the power of which was a linear model of CPU utilization percentage.

3. Proposed secure virtual machine migration Methodology

VM migration is mainly used for providing high availability, hardware maintenance, workload balancing and fault takeover in Cloud environment. Migration is one of the useful features of Virtualization technology which is used to transfer a VM from one physical server to another or from one data centre to another. However it is vulnerable to active and passive security attacks during the migration process, which makes IT industry hesitant to accept this feature in Cloud. Compromising on VM migration process may result in Denial of Service (DOS) attacks, loss of data integrity and confidentiality. To cater different attacks such as unauthorized injecting malicious code on VM disk, the cloud providers store the information in encrypted form. Therefore security of VM migration along encryption becomes necessary. To solve this issue the proposed method consider security aware VM migration through optimal cryptography algorithm. Optimal cryptography is a combination of sanitization algorithm and Orthogonal Learning Particle Swarm Optimization (OLPSO) algorithm. The proposed optimal cryptography algorithm will increase the confidentiality of the migrated data. Flow diagram of the implemented method is shown in fig.1.

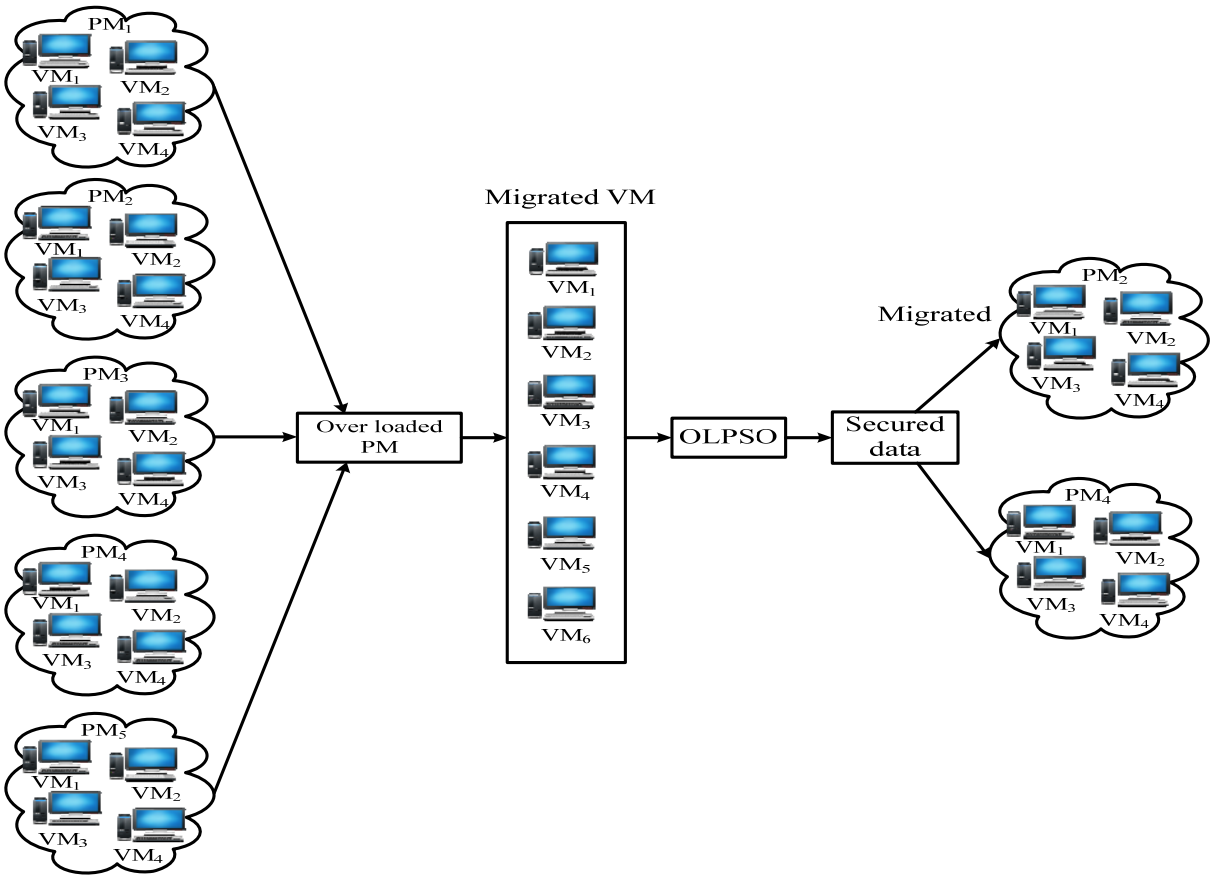


Fig.1 Flow diagram of implemented method

Consider a cloud network containing n number of Physical machines (PMs) and each PM consists of m number of VMs. Each task T is randomly assigned to a different VM. In this paper the objective function is based on VM components such as energy, migration cost, and memory utilization. The problem can be formulated by using equation (1).

$$FitnessFunction = Min\left[\lambda_1(E)+\lambda_2(MC)+\lambda_3(M)\right] \quad (1)$$

Where E is energy efficiency, MC is Migration Cost, M is memory utilized.
Depends on this fitness function the tasks moves to another VM. As a result the migration of VM happens and data should be secured. So the proposed method designed for secure VM migration scheme with the help of optimal cryptography algorithm.

3.1 Sanitization algorithm

The proposed optimal cryptography algorithm is used to increase the confidentiality of the migrated data. Here the sanitization algorithm and OLPSO algorithm is combined for more security. The optimal sanitization process is given in figure 2. The detailed explanation of optimal cryptography algorithm is described beneath.

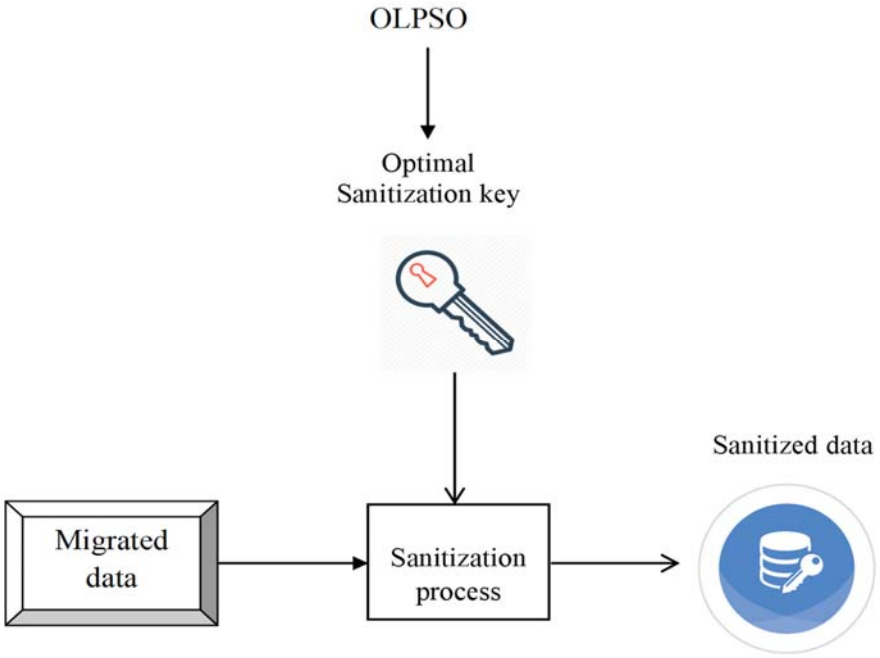


Figure 2: Optimal sanitization process

3.1.1 Sanitization

Sanitization is an important privacy measure when releasing and sharing sensitive datasets. Data Sanitization is a type of information sanitization whose intention is to protect privacy. It is the process of encrypting sensitive information from data sets so that the people whom the data describe remain anonymous. It has been defined as technology that converts clear text data into a nonhuman readable and irreversible form.

For example, sanitization is a mathematical operation on two functions D and ξ, producing encrypted data that is typically viewed as a modified version of one of the original functions. Let $D(t)$ and $\xi(t)$ be two functions. The sanitization of $D_{a\times b}$ and $\xi_{a\times b}$, denoted by $E^*_{a\times b}$ is given by:

$$E^*_{a\times b} = \left(D_{a\times b} \otimes \xi_{a\times b}\right) \quad (2)$$

$E^*_{a\times b}$ – *Encrypted Data or Sanitized Data*

$D_{a\times b}$ – *Original Data*

$\xi_{a\times b}$ – *Key*

$a\times b$ – *Size of matrix*

From the above process, the input task is encrypted and then the migration process is done in the proposed method. In the proposed sanitization process, the key is generated for all data. Initially random prime numbers $K_i = (K_1, K_2, ...K_n)$ are selected for a key generation process. In order to secure the data the suggested method has to select the optimal key or best key. For that purpose, orthogonal learning particle swarm optimization (OLPSO) algorithm is used to generate optimal key for each input data.

3.1.2 Orthogonal Learning Particle Swarm Optimization (OLPSO) Algorithm

OLPSO is mainly concentrated on three main components of the algorithm such as personal best experience, the global best experience and the worst experience of the respective particles. In OLPSO the particle u is spread in a dimensional space. Each particle u is associated with respective position and velocity. The current state of velocity is A_u and the current position vector is B_u. The vectors A_u and B_u are modified randomly and updated in the following equations.

$$A_u^* = \omega A_u + c_1 r_1 (P_u - B_u) + c_2 r_2 (P_n - B_u) \quad (3)$$

$$B_u^* = B_u + A_u \quad (4)$$

ω → Inertia weight.

c_1 *and* c_2 → Randomly selected value which is fixed to be 2.0.

r_1 *and* r_2 → Random value consistently generated inside the interval [0, 1].

P_u → Personal best position.

P_n → Position of neighborhood particle.

OLPSO combines information P_u and P_n to form a better guidance vector P_G . To form an enhanced guidance vector P_G the original PSO can be adapted with an Orthogonal Learning approach that joins information of P_u and P_n . The particle's flying velocity is

$$A_u = \omega A_u + cr(P_G - B_u) \quad (5)$$

The guidance vector P_G is constructed for each particle u.

$$P_o = P_u \oplus P_n \quad (6)$$

Where

P_u → Personal best position

P_n →Neighborhood's best position

$\oplus$ → Stands for cooperative operation

3.1.3 Step by step process of key generation using optimal cryptography.

For security purpose the optimal sanitization approach is used. Sanitization process is used for encryption process and for key generation process optimization algorithm is utilized. The step by step process of key generation is explained below.

Initialization: The position of the candidate solution is initialized in a *d* dimensional space vector. In this approach random prime numbers or private keys are considered as the candidate solutions in the range [1, n-1]. It can be initialized as follows.

$$Y_k(t) = \{Y_{k1}(t), Y_{k2}(t), ...Y_{kd}(t)\} \quad (7)$$

$Y_{kd}(t)$ - is the population of the solutions in the d^{th} dimension vector. The population of this algorithm at iteration't' is considered as follows.

$$Y(t) = \{y_1(t), y_2(t), ...y_n(t)\} \quad (8)$$

Where $y_n(t)$ represent the position of the i^{th} candidate in the solutions.

Fitness evaluation: To evaluate the optimal solution the fitness value is to be calculated for the initialized solutions. For optimal key selection the fitness is defined based on the throughput of solution in this approach. The throughput of the solution is defined as the ratio between the size of the plaintext in bytes and the encryption time in seconds. It can be calculated as follows.

$$T_k(t) = \frac{Size\ of\ plain\ \ text}{Encryption\ time} \tag{9}$$

Where $T_k(t)$ represents the throughput of the k^{th} solution. Using equation (10) fitness function of the solution is calculated.

$$Fit_k(t) = Max(T_k(t)) \tag{10}$$

The solution with the maximum fitness value is selected as the optimal solution. Then the best and worst fitness of the solutions or populations is sorted. Each solution is updated until finding the optimal solution.

After the fitness calculation each particle is updated their velocities and positions according to (11) and (12).

$$A_u = \omega A_u + cr(P_G - B_u) \tag{11}$$

$$B_u^* = B_u + A_u \tag{12}$$

Termination: The above process is stopped until finding the optimal solution or private key ($K_{Optimal}$) from the initial solution. Once the optimal solution is attained the algorithm will be terminated.

Based on the above process the optimal key values are generated. Then the resultant output is fed to the cryptography process. The proposed cryptography method is a mathematical way of combining data and optimal key to form an encrypted data. During migration the virtual machine sends the input data and the optimal key value to the sanitization process.

3.2 Migration

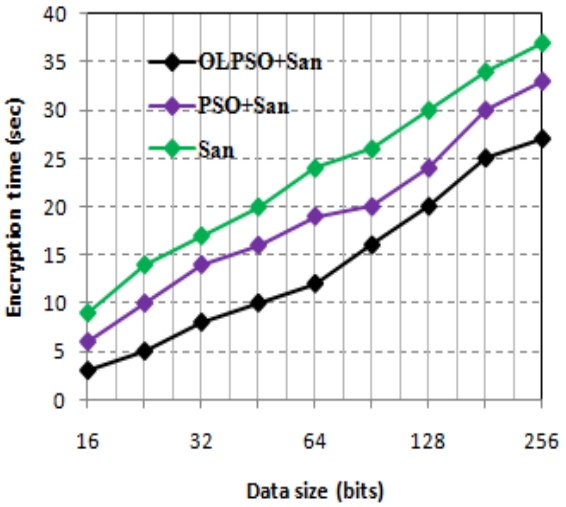
After the encryption process the VM is migrated to under loaded host in which we can able to save the energy.

4. Result and discussion

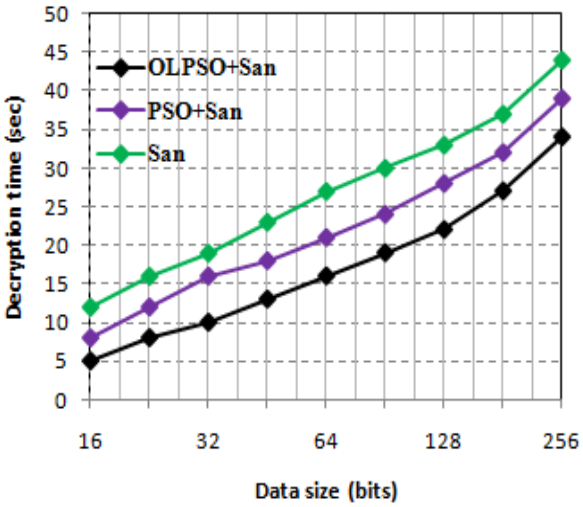
In the proposed methodology experimental results are analyzed and performance is analyzed in terms of different evaluation metrics. The proposed approach is implemented in JAVA.

4.1.1 Experimental results based on security process

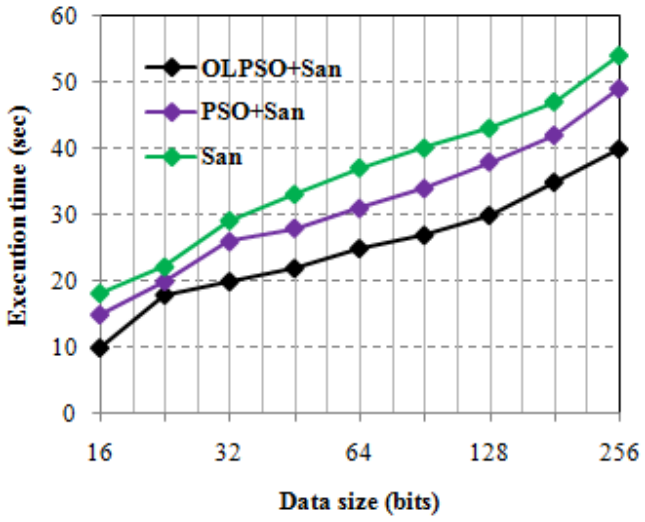
For the encryption process the optimal cryptography algorithm is utilized which is a combination of sanitization algorithm and OLPSO. Sanitization is used to encrypt the data and OLPSO is used for key generation process. The best key is selected with the help of fitness function. The maximum throughput is considered as the fitness function.



(a)



(b)



(c)

Figure 3. Time analysis for security model (a) encryption time (b) decryption time and (c) Execution time.

Figure 3 shows the time analysis for security models. In the proposed security model the graph is drown for encryption time, decryption time and execution time based on data sizes. Evaluated the performance in different data sizes such as 16, 32, 64, 128 and 256. The proposed approach is taken minimum time to encrypt data compared to other two algorithms. Similarly in figure 3(b) the performance of decryption time is analyzed. For security, in this paper optimal sanitization approach is utilized. In this key optimization OLPSO algorithm is used. OLPSO algorithm speeds up the execution process. So that, we took minimum time to execute the security process. When analyzing figure 3(c) it clearly understands the proposed approach is taken minimum time to complete the process.

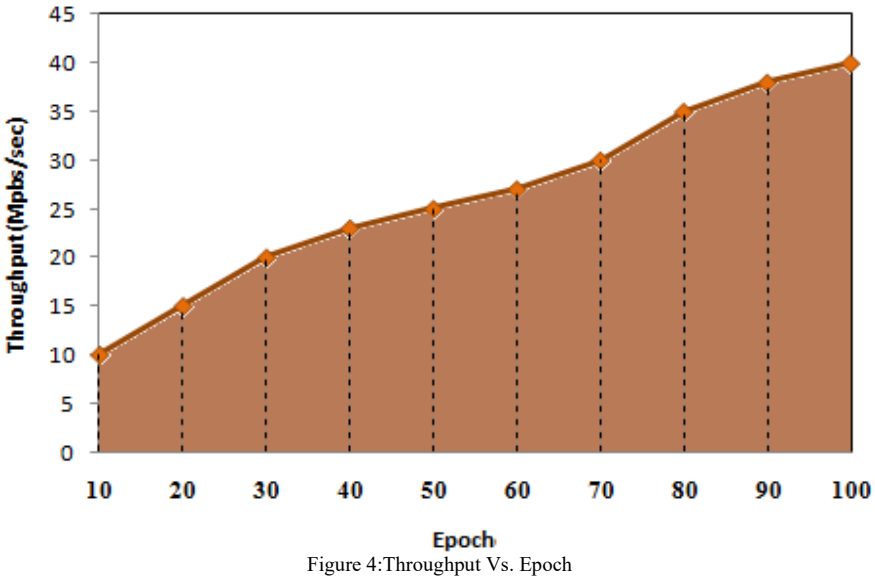
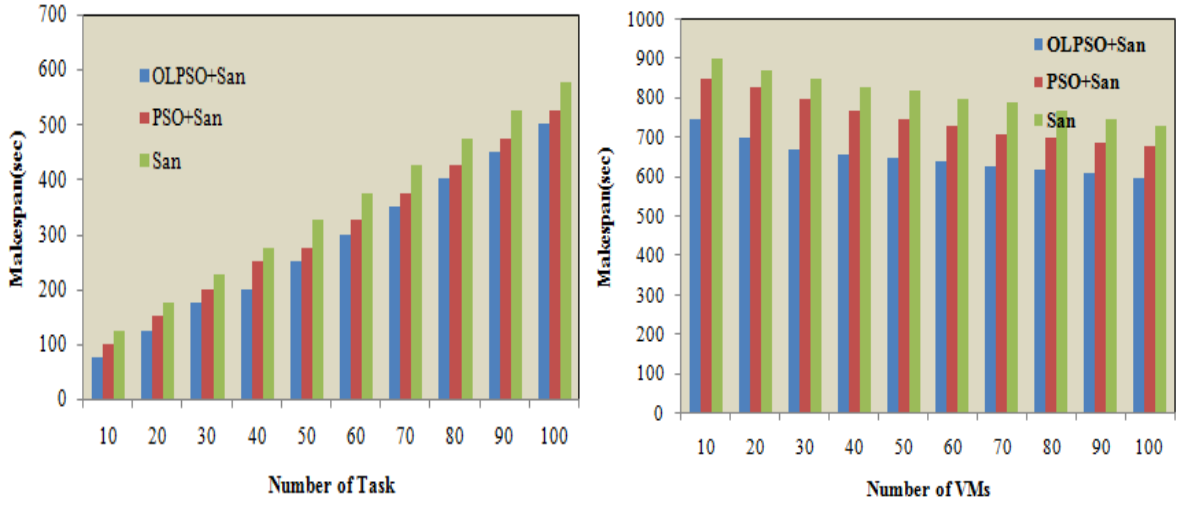


Figure 4:Throughput Vs. Epoch

The objective analysis of optimization appears in figure 4 by shifting the number epoch, the most extreme throughput is 40Mbps/sec in 100 Epoch of Swarm optimization process. This is plotted regarding time period.

4.1.2 Experimentation results based on the migration process

Migration process consumes the energy of the system**.** The process is evaluated in terms of different metrics namely make span and energy consumption. The good system provides the less make span and energy consumption.



(a) (b)

Figure 5.Comparison of make span of the system using different algorithms (a) number of VM is fixed and task varies (b) number of task is fixed and VM varies.

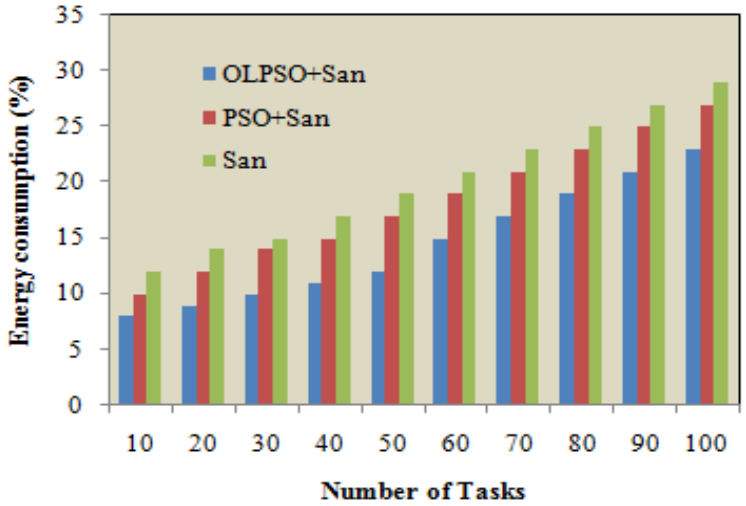


Figure 6: Comparison of energy consumption by varying number of tasks

In figure 5(a) the number of VM is set to 50, and the number of tasks increases from 10 to 100 in the gap of 100. Here, the x-axis represents the number of task and y-axis represents the make span. As the number of task increases make span also increases. In figure 5(b) the number of task is set to 100, and the number of VM increases from 10 to 100 in the gap of 10. When analyzing the proposed method attains the minimum make span compared to other methods. Moreover, a comparison of energy consumption of the system by varying number of task is given in figure 6. The x-axis represents the number of task and y-axis represents the energy consumption. As the number of task increases energy also increases. From the results it is clearly understood that the proposed algorithm got better performance compared to other methods.

5. Conclusion

Energy efficient secure virtual machine migration using optimal cryptography method has been introduced in this paper. For security purpose the data migrated data has been migrated with the help of optimal sanitization approach. The key value of sanitization algorithm has been selected with the help of OLPSO algorithm. The mathematical explanation of OLPSO and sanitization algorithms has been explained properly. The experimental results are analyzed in terms of different metrics. Compared to the existing algorithms the proposed method attain the minimum make span and energy consumption. As a future scope this findings can be implemented in real time data.

References.

[1] Nelson, Michael, Beng-Hong Lim, and Greg Hutchins. "Fast Transparent Migration for Virtual Machines." In USENIX Annual technical conference, general track, pp. 391-394. 2005.
[2] Fan, Wei, Zhujun Zhang, Tingting Wang, Bo Hu, Sihan Qing, and Degang Sun. "Research on security algorithm of virtual machine live migration for KVM virtualization system." In International Conference on Information and Communications Security, pp. 54-70. Springer, Cham, 2016.
[3] Zhang, Fengzhe, and Haibo Chen. "Security-preserving live migration of virtual machines in the cloud." Journal of network and systems management 21, no. 4 (2013): 562-587.
[4] Uchibayashi, Toshihiro, Bernady Apduhan, Takuo Suganuma, and Masahiro Hiji. "Toward a Secure VM Migration Control Mechanism Using Blockchain Technique for Cloud Computing Environment." In International Conference on Computational Science and Its Applications, pp. 177-186. Springer, Cham, 2018.
[5] Zeb, Tayyaba, Abdul Ghafoor, Awais Shibli, and Muhammad Yousaf. "A Secure Architecture for Inter-cloud Virtual Machine Migration." In International Conference on Security and Privacy in Communication Networks, pp. 24-35. Springer, Cham, 2014.
[6] Vaezi, M., & Zhang, Y. (2017). Virtualization and Cloud Computing. In Cloud Mobile Networks (pp. 11-31). Springer International Publishing.
[7] Wood, Timothy, Prashant J. Shenoy, Arun Venkataramani, and Mazin S. Yousif. "Black-box and Gray-box Strategies for Virtual Machine Migration." In NSDI, vol. 7, pp. 17-17. 2007.
[8] Jin, Hai, Li Deng, Song Wu, Xuanhua Shi, and Xiaodong Pan. "Live virtual machine migration with adaptive, memory compression." In 2009 IEEE International Conference on Cluster Computing and Workshops, pp. 1-10. IEEE, 2009.
[9] Akoush, Sherif, Ripduman Sohan, Andrew Rice, Andrew W. Moore, and Andy Hopper. "Predicting the performance of virtual machine migration." In 2010 IEEE international symposium on modeling, analysis and simulation of computer and telecommunication systems, pp. 37-46. IEEE, 2010.
[10] Zhang, Fengzhe, and Haibo Chen. "Security-preserving live migration of virtual machines in the cloud." Journal of network and systems management 21, no. 4 (2013): 562-587.
[11] Garfinkel, Tal, and Mendel Rosenblum. "When Virtual Is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments." In HotOS. 2005.
[12] Li, Chunxiao, Anand Raghunathan, and Niraj K. Jha. "Secure virtual machine execution under an untrusted management OS." In 2010 IEEE 3rd International Conference on Cloud Computing, pp. 172-179. IEEE, 2010.
[13] Jarraya, Yosr, Arash Eghtesadi, Sahba Sadri, Mourad Debbabi, and Makan Pourzandi. "Verification of firewall reconfiguration for virtual machines migrations in the cloud." Computer Networks 93 (2015): 480-491.
[14] Jayant Baliga, Robert W. A. Ayre, Kerry Hinton, and Rodney S. Tucker, "Green cloud computing: Balancing energy in processing, storage, and transport." Proceedings of the IEEE, Vol. 99, No.1, pp. 149-167, 2011.
[15] Paulraj, Getzi Jeba Leelipushpam, Sharmila Anand John Francis, J. Dinesh Peter, and Immanuel Johnraja Jebadurai. "Resource-aware virtual machine migration in IoT cloud." Future Generation Computer Systems 85 (2018): 173-183.
[16] Paulraj, Getzi Jeba Leelipushpam, Sharmila Anand John Francis, J. Dinesh Peter, and Immanuel Johnraja Jebadurai. "A combined forecast-based virtual machine migration in cloud data centers." Computers & Electrical Engineering 69 (2018): 287-300.
[17] Dévigne, Clément, Jean-Baptiste Bréjon, Quentin L. Meunier, and Franck Wajsbürt. "Executing secured virtual machines within a manycore architecture." Microprocessors and Microsystems 48 (2017): 21-35.
[18] Noshy, Mostafa, Abdelhameed Ibrahim, and Hesham Arafat Ali. "Optimization of live virtual machine migration in cloud computing: A survey and future directions." Journal of Network and Computer Applications 110 (2018): 1-10.
[19] Zhao, Ming, and Renato J. Figueiredo. "Experimental study of virtual machine migration in support of reservation of cluster resources." In Proceedings of the 2nd international workshop on Virtualization technology in distributed computing, p. 5. ACM, 2007.
[20] Huang, Qiang, Fengqian Gao, Rui Wang, and Zhengwei Qi. "Power consumption of virtual machine live migration in clouds." In 2011 Third International Conference on Communications and Mobile Computing, pp. 122-125. IEEE, 2011.

Author details:

Nimmol P. John received her Master's Degree in Computer Management from Chh.Shivaji University, Kolhapur, India. Presently, she is a research scholar in School of Computer Sciences, Mahatma Gandhi University, Kerala, India. Her research interests include Cloud Computing and Design and Analysis of Algorithms.

Dr. Bindu V R received her Master's Degree in Computer Science from University of Kerala, India and Ph.D degree in Computer Science from Mahatma Gandhi University, India. She joined School of Computer Sciences, Mahatma Gandhi University, Kerala, India in 1993 and is currently Professor and Dean , Faculty of Science, Mahatma Gandhi University. Her research interests include Digital Image Processing and Computer Vision, Machine Learning and Artificial intelligence, Cloud Computing and Data Science. She has authored more than 40 research papers in reputed international journals and conference proceedings.