Advances in Computational Sciences and Technology
ISSN 0973-6107 Volume 10, Number 8 (2017) pp. 2541-2553

http://www.ripublication.com

A Secured and Enhanced Energy Efficient Solution for Cloud Computing Environment

Anupama Gupta[1], Vivek Aggarwal[2*], Ramandeep Singh Dhillon[3]

[1,3] Lala Lajpat Rai Institute of Engineering and Technology, Moga-142001, Punjab, India.

[2] I. K. Gujral Punjab Technical University, Main Campus, Kapurthala, Punjab, India.

Abstract

Owing to the requirement of energy savings, several approaches to location sensing based energy-efficient solutions have been explored. These approaches make assumptions about the user activity and generally reduce either the accuracy requirements or aggressively use other signals to determine when and where to turn on Evolutionary Algorithm. Moreover, the concerns like security, power consumption, service level agreement violation, performance degradation due to virtual machine task migration and optimization have still not been addressed completely. In this work, the virtual machine has been designed in such a way that tasks can be achieved using better service level agreement and less energy. To accomplish this, an enhanced Evolutionary Algorithm has been designed and implemented for minimizing power consumption without making significant modifications over the other areas to meet quality of Infrastructure as a Service. The security of this system is provided by applying the Fast Encryption Algorithm on binary images and text data.

Index Terms: Cloud Computing, Encryption, Energy Consumption, Infrastructure-as-a-Service, Security, Virtual Machine

I. INTRODUCTION

Cloud computing also sometimes known as utility computing enables convenient and on-demand network access to a large number of computing resources such as network, software, storage, applications and services from anywhere across the globe with a negligible effort and interaction of service provider. It has become indispensable in the preparation of many cloud infrastructures [1]. The basic principle of cloud computing is to use the virtualization technology to provide the desired services from shared hardware with the aim of creating a much better use of distributed resources. The environment of cloud computing incorporates many existing technologies and infrastructure consisting of masses of computers, distributed applications, information, storage and network resources. Cloud computing is generally categorized into three cloud service models, namely *Software as a Service* (SaaS), *Platform as a Service* (PaaS) and *Infrastructure as a Service* (IaaS) [2]. These cloud models are depicted in Fig. 1. In *Software as a Service* (SaaS) model, the end users exploit the applications running on cloud infrastructure from mobile devices or browsers on a rental or per use basis. Typical examples include Microsoft Office 365, Google apps, Salesforce.com, etc. In *Platform as a Service* (PaaS) model, the services like core operating system and building block services are made available to end users so that they can run their applications. Examples in this category include Windows Azure, Google App Engine, Force.com, etc. In *Infrastructure as a Service* (IaaS) model, the cloud vendors offer components of infrastructure like load balancers, storage, networks, processor, memory, virtualization, etc. to the end users for a specific time and price on an agreed basis. Examples of IaaS include Amazon EC2, Microsoft Azure Platform, Cisco Metapod, etc.

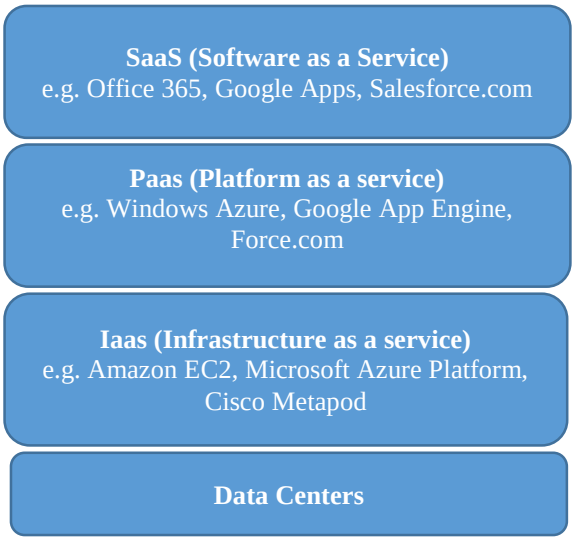

Fig. 1. Different cloud service models

Data Centers lay the foundation of cloud computing. These generally consist of thousands of servers which are connected to each other and are built in less occupied area with inexpensive energy rates [3-5].

The focus of this paper is on designing the virtual machine (VM) in a way that allows the tasks to be achieved using better service level agreement, and minimum energy to meet quality of Infrastructure as a Service. For this purpose, an enhanced evolutionary algorithm has been designed and implemented. The security of the system has been provisioned using Fast Encryption Algorithm on images and text data. The paper is organised as follows. Section II provides an overview of the related work carried out in the direction of VM power consumption and placement. Section III presents the architecture of the proposed work. In Section IV, the proposed methodology has been discussed. Section V presents the results and discussion. Finally, Section VI discusses the conclusions and scope for future work.

II. RELATED WORK

Several techniques have been proposed in past to address the problems to measure the power consumption of each VM and securing the data transfer across cloud. Some of these techniques proposed by different authors have been outlined below:

Wang et al. [6] considered the problem of ensuring integrity of data stored on cloud servers. The authors achieved data integrity while allowing both public verifiability of data through third party auditor and dynamic data operations such as block modification, deletion, insertion, etc. on behalf of end users.

Yu et al. [7] addressed the security challenges for data security and access control by incorporating access policies which were based on data attributes and allowing end users to delegate the computational overheads involved in access control to untrusted servers. The approaches of attribute-based encryption, lazy re-encryption and proxy re-encryption were explored and combined in a unique manner. The proposed scheme proved to be highly secure and efficient under prevailing security models.

Subashini et al. [8] carried out a survey of different security risks prevalent in the cloud service models. Authors emphasized that though there were numerous advantages in using a cloud architecture, yet, the issues like service level agreement, security, power consumption, accuracy, etc, remain unresolved.

Beloglazov et al. [9] proposed the energy-aware resource allocation algorithms utilizing the dynamic consolidation of virtual machines. The architectural principles for energy-efficient management of clouds, resource allocation policies and scheduling algorithms were put forward keeping in mind the desired quality-of-service parameters and power consumption features of varying devices. The results revealed that in comparison to static resource allocation techniques, the proposed technique efficiently reduced energy consumption in cloud data centres.

Li et al. [10] described that owing to heterogenous nature of jobs, different VMs have different job completion times even on same physical machine. Moreover, the physical

machines are heterogeneous in nature. Therefore, VM placement times on them also vary. Authors suggested an off-line VM placement schedule using emulated VM migration and an on-line VM placement method through a real VM migration process. The results validated that the proposed algorithm was highly efficient in placement of VMs.

Zhang et al. [11] implemented and deployed VM Thunder technology to address the problem faced by cloud service providers in provisioning several VMs to meet end users' computing needs. The VMThunder technology is a new VM provisioning tool which is based on the observation that when a guest VM starts, the data blocks accessed by the VM follow a specific pattern. Moreover, the same type of VMs retrieves comparable data blocks during the booting process regardless of their configuration settings. The experimental results showed that VMThunder proved to be powerful VM provisioning tool in terms of latency, scalability, and I/O performance for IaaS cloud.

Gu et al. [12] proposed a VM power metering tree regression-based technique for measuring the power consumed by VMs while they were competing for resources on the same server. The method recursively split the input dataset into two subsets depending on the selected resource feature such as CPU, cache, etc. The proposed method proved to be appropriate for real time use and quite effective power management tool for green cloud data centers. The results showed that the accuracy of the method was nearly 98% for diverse kinds of applications running in VMs.

Li et al. [13] described that VM allocation problem for multiple tenants in cloud data centers is a NP hard problem. Authors proposed a layered progressive resource allocation algorithm based on the multiple knapsack problem (LP-MKP). The algorithm adopted the minimization of the sum of the VMs' network diameters of all tenants as optimization goal and attempted to lower the resource fragmentation in cloud environment, reduced the differences in the Quality-of-Service (QoS) among different tenants and enhanced the overall Quality-of-Service. The results clearly showed that the proposed algorithm effectively and efficiently resolved the multi-tenant VM resource allocation problem in cloud data centers.

Chowdhury et al. [14] designed and implemented multiple VM placement algorithms to solve the problem of energy consumption and performance requirements for meeting the quality of Infrastructure-as-a-service. Authors used heuristics for consolidation of virtual machines based on previous resource usage data. Both underloaded and overloaded hosts were detected and bin packing solutions were proposed to address the problem of placement of multiple VM instances on a single host machine for maximizing the resource utilization and increasing the return on investment. The results of simulation demonstrated that the proposed techniques, especially, the modified worst fit decreasing virtual machine placement approach performed significantly better than the existing virtual machine placement algorithm designed in CloudSim.

Dong et al. [15] introduced greedy task scheduler to investigate energy efficient task scheduling for cloud data centres. The task assignment was formulated as integer-programming problem to reduce the energy consumption by cloud data servers by proposing the most-efficient-server-first task-scheduling scheme. Simulation results

showed that the energy consumption using proposed scheduling scheme was 70 times lesser than the one based on random-based task-scheduling scheme.

III. ARCHITECTURE OF PROPOSED WORK

Apart from number of solutions that have been put forward to reduce power consumption for cloud data centres and improve service level agreement, the proposed approach assumes that the IaaS cloud has diverse computing nodes which are classified to make clusters. For each node, there is an associated special software package known as virtualization whose main operation is to create and maintain the virtual machines. Additionally, it fulfils the requests of the end users for accessing the desired resources by enabling the isolation and abstraction of underlying hardware and low-level functionalities in the cloud. There is a set of end user tasks each of which may have several subtasks. A subtask is allocated to a resource at a time and resources are available continuously. The aim is to remove the virtual machines from underloaded hosts so that they can be shut to save the power and reduce the operational cost. It is also desirable to migrate the virtual machines from overladed hosts so that the performance is not degraded. To accomplish this, an improved Evolutionary Algorithm has been used due to its powerful search capability, global solution finding feature and compact structure with few parameters [16-17]. The proposed approach is compared against the modified worst fit decreasing virtual machine placement (MWFDVP) approach explored by Chowdhury et al. [14] in their comparison work on multiple VM placement algorithms. The MWFDVP prefers the host machine with highest gain in consumption of energy because according to them, the merits of worst-fit heuristics outweigh the best-fit heuristics.

The proposed algorithm begins with random selection of initial parameters to constitute the individual vectors which then go through mutation process. Every individual vector becomes a target vector for which mutation operation is applied to eventually produce a mutant vector. The crossover operation is applied to recombine mutant vector with the parent. The fitness function evaluates and selects the child for next generation. The objective is to determine better quality descendants which will feed the next generation and permit the search operation to explore those areas of solution space which have not been explored before. The security has been provided using a fast encryption algorithm which is based on Data Encryption Standard (DES) [18-20]. The traditional encryption-decryption algorithms are slow because in both the stages of permutation and diffusion, the image is analyzed twice which takes quite a lot of time. This limitation has been overcome in the present work. The present encryption scheme uses symmetric key cryptography and works on 64-bit blocks. The data is first divided into blocks which are then shuffled and some random numbers are generated from that to further enhance the encryption. The sender encrypts the message using shared key which is decrypted by the receiver of the message using the same key. It provides high speed security to the messages delivered over the cloud.

IV. METHODOLOGY AND FLOW OF WORK

The flow graph for the proposed work is shown in Fig. 2. First, the virtual machines are placed on the host after verifying the resource vectors of both host as well as the virtual machines.

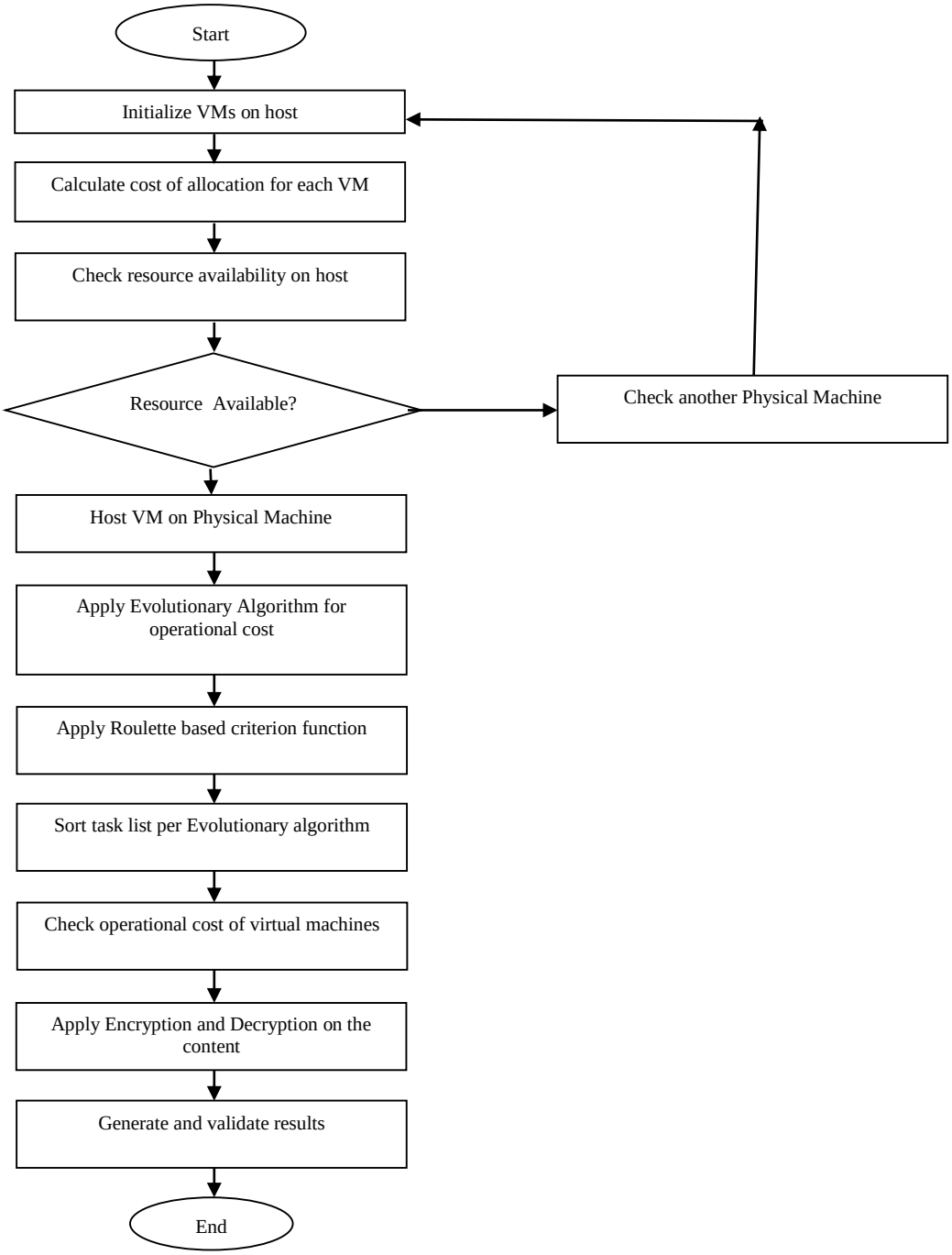

Fig. 2. Flowchart of the proposed work

If adequate resources are available on the host, then VM will be placed on that host. After VM placement, the task allocation on the VM is done. The aim is to reduce the operational cost expended for assignment of tasks on VM. To accomplish this, proposed Evolutionary Algorithm is implemented which sorts the tasks and places them on the suitable VM according the Roullet based criterion function. Subsequently, the operational cost is calculated. After applying Evolutionary algorithm, the security is envisioned using Fast Encryption Algorithm to protect the data from attackers. Next, the results are generated and compared to existing algorithm [14] to validate the proposed research.

There are eight host machines on which many virtual machines can be deployed (Fig. 3). The task list is stored on the virtual machines and operations are performed accordingly. The encryption is done on the text and the binary data. The proposed algorithm works in following stages:

Fig. 3. Graphical user interface for the proposed scheme

a. Initially, the virtual machines are in idle state and no load is assigned to them.
b. Subsequently, the task list is fed and the overloaded condition is shown. Whenever a machine is in the overloaded condition, the color of that machine changes to red (Fig. 4). The threshold value for overloading is set to 80% of CPU utilization.

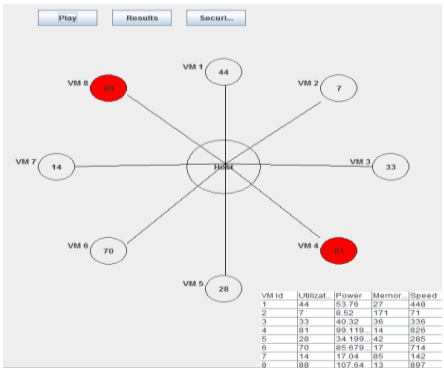

Fig. 4. Overloaded Hosts

c. The security is provided using Fast Encryption Algorithm (FEAL) which is an extension of DES encryption algorithm. It is applied to both plain text and binary data.
d. Several security attacks, for example, brute force attack, are performed on cloud to check if it is robust against attacks or not (Fig. 5).

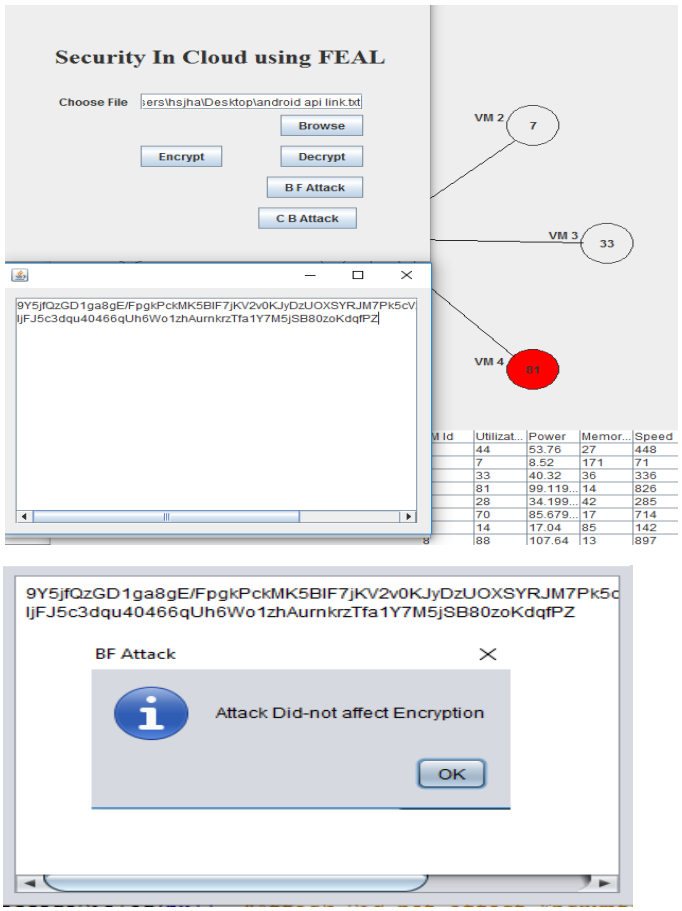

Fig. 5. Encrypted Data before and after subjecting to attacks

e. After the encryption of data on the cloud, the decryption process comes into play. The plain text is decrypted to a readable format. It is seen that the encrypted text is robust enough against the attacks on security.
f. After all the successful operations on the plain text, the encryption and decryption of binary data, i.e., images are performed. The images are subdivided into blocks and then, block ciphers are produced and transmitted across cloud.
g. The algorithm also shows the location of the specific node on which the file is encrypted (For example, node 5 in the present case) and is stored subsequently (Fig. 6).

h. Finally, the results are generated, compiled and validated using four quantitative metrics, namely, CPU utilization, power utilization, efficiency and over utilization.

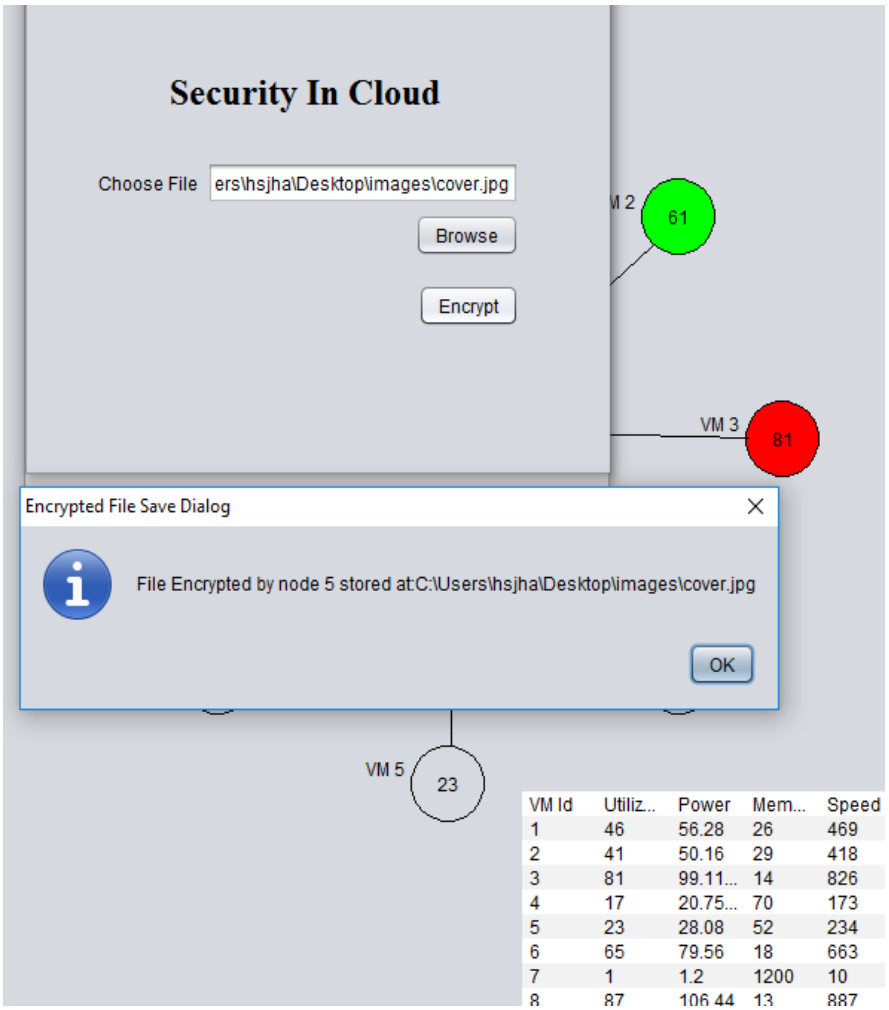

Fig. 6. Location of encrypted file

V. RESULTS AND DISCUSSION

The proposed algorithm is executed in the CloudSim which is a cloud computing simulation toolkit. The results are generated and compared with the Modified Worst Fit Decreasing Virtual Machine Placement (MWFDVP) approach in terms of power utilization, CPU utilization, efficiency and over-utilization. Fig. 7 and Fig. 8 show power consumption and CPU utilization respectively, using MWFDVP and proposed approaches. The cloudlet size parameter is taken on x-axis which is increased up to 80 to check out the scalability of the approach.

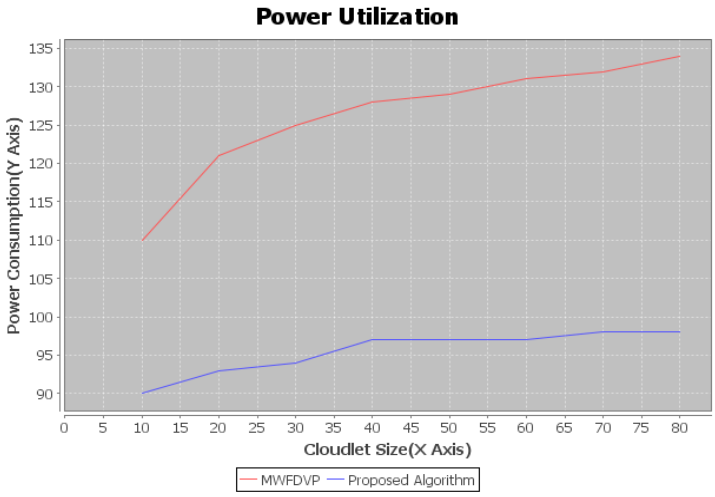

Fig. 7. Power Consumption vs Cloudlet Size for MWFDVP and proposed approaches

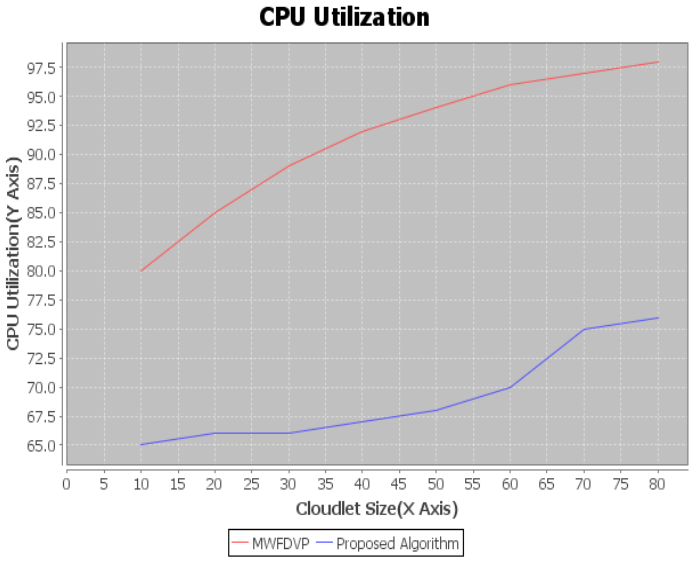

Fig. 8. CPU Utilization vs Cloudlet Size for MWFDVP and proposed approaches

Both the graphs (Fig. 7 and Fig. 8) clearly depict that the use of proposed scheme significantly reduces power consumption and CPU utilization in comparison to the Modified Worst Fit Decreasing Virtual Machine Placement (MWFDVP) approach. Fig. 9 shows how the efficiency of resources is increased using the proposed approach. On the x-axis, the number of hosts are defined which are increased up to 5 to check out the scalability of the approach where as on the y-axis, the efficiency parameter is defined.

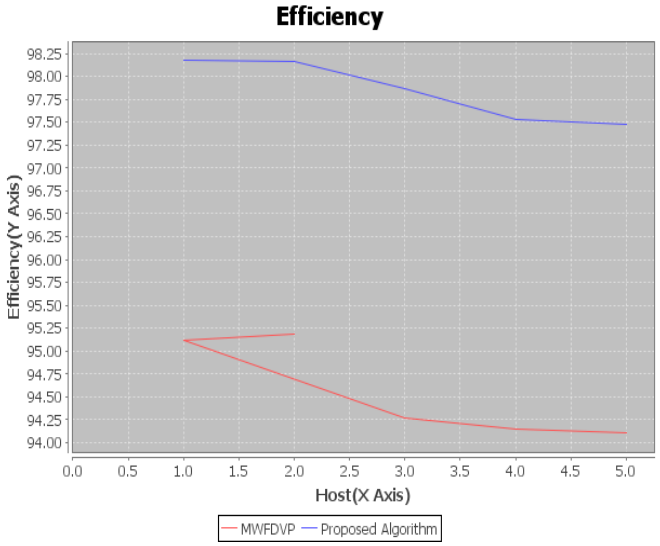

Fig. 9. Efficiency vs Number of Hosts for MWFDVP and proposed approaches

Fig. 10 depicts how over utilization of resource vector using proposed approach is reduced. On the x-axis, the number of virtual machines are shown which is increased up to 50 to check out the scalability of the approach, whereas, on the y-axis, the over utilization parameter is shown.

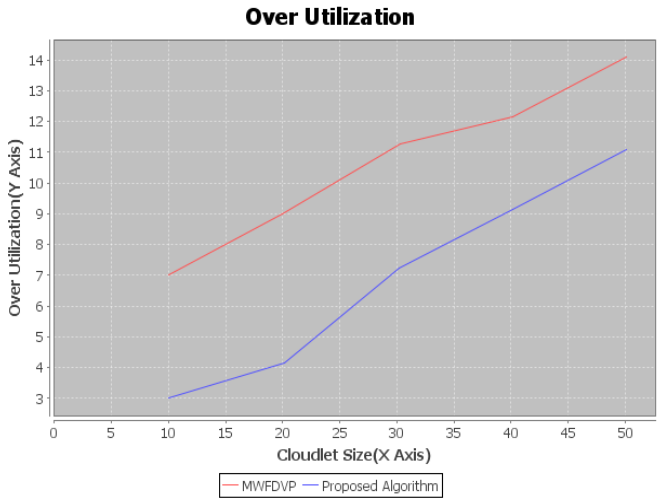

Fig. 10 Over Utilization vs Cloudlet Size for MWFDVP and proposed approaches

VI. Conclusions and Future Scope

Today security is the main concern that hampers the growth of the cloud computing. Several approaches of providing secure and energy efficient solutions for cloud computing frameworks have been put forward, however, most of the attention has been focussed on addressing only one concern. In the present work, an attempt has been made by proposing an enhanced algorithm that can add security to the cloud environment and at the same time, can help in lowering power consumption. The experimental results validate the proposed algorithm. In future, the proposed scheme may be further optimized to a single algorithm to achieve better VM placement, task assignment and reduced power consumption with added security.

REFERENCES

[1] R. Buyya, R. Ranjan, and R. Calheiros, "Intercloud: Utility-oriented federation of cloud computing environments for scaling of application services," *Algorithms and architectures for parallel processing*, pp. 13-31, 2010

[2] W. T. Tsai, X. Sun, and J. Balasooriya, "Service-oriented cloud computing architecture," in IEEE Seventh International Conference on Information Technology: New Generations (ITNG), pp. 684-689, April 2010.

[3] Y. Jadeja and K. Modi, "Cloud computing-concepts, architecture and challenges," in IEEE International Conference on Computing, Electronics and Electrical Technologies (ICCEET), pp. 877-880, March 2012.

[4] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches", *Wireless communications and mobile computing*, vol. 13, no. 18, pp. 1587-1611, 2013.

[5] W. Kim, "Cloud computing architecture", *International Journal of Web and Grid Services*, vol. 9, no. 3, pp. 287-303, 2013.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing", in European symposium on research in computer security, pp. 355-370, September 2009. Springer Berlin Heidelberg.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing", in IEEE proceedings of Infocom, pp. 1-9, March 2010.

[8] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", *Journal of network and computer applications*, vol. 34, no. 1, pp. 1-11, 2011.

[9] A. Beloglazov, J. Abawajy, and R. Buyya, "Energy-aware resource allocation heuristics for efficient management of data centers for cloud computing",

Future generation computer systems, vol. 28, no. 5, pp. 755-768, 2012.

[10] K. Li, H. Zheng, and J. Wu, "Migration-based virtual machine placement in cloud systems", in IEEE 2nd International Conference on Cloud Networking (CloudNet), pp. 83-90, November, 2013.

[11] Z. Zhang, Z. Li, K. Wu, D. Li, H. Li, Y. Peng, and X. Lu, "VMThunder: fast provisioning of large-scale virtual machine clusters", *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 12, pp. 3328-3338, 2014.

[12] C. Gu, P. Shi, S. Shi, H. Huang, and X. Jia, "A tree regression-based approach for VM power metering", IEEE *Access*, vol. 3, pp. 610-621, 2015

[13] J. Li, D. Li, Y. Ye, and X. Lu, "Efficient multi-tenant virtual machine allocation in cloud data centers", *Tsinghua Science and Technology*, vol. 20, no. 1, pp. 81-89, 2015.

[14] M. R. Chowdhury, M. R. Mahmud, and R. M. Rahman, "Implementation and performance analysis of various VM placement strategies in CloudSim", *Journal of Cloud Computing*, vol. 4, no. 1, pp. 20, 2015

[15] Z. Dong, N. Liu, and R. Rojas-Cessa, "Greedy scheduling of tasks with time constraints for energy-efficient cloud-computing data centers", *Journal of Cloud Computing*, vol. 4, no. 1, pp. 5, 2015.

[16] K. Dasgupta, B. Mandal, P. Dutta, J. K. Mandal, and S. Dam, "A genetic algorithm (GA) based load balancing strategy for cloud computing", *Procedia Technology*, vol. 10, pp. 340-347, 2013

[17] E. Zitzler, K. Deb, and L. Thiele, "Comparison of multiobjective evolutionary algorithms: Empirical results", *Evolutionary computation*, vol. 8, no. 2, pp. 173-195, 2000.

[18] Y. Wang, K. W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm", *Applied soft computing*, vol. 11, no. 1, pp. 514-522, 2011.

[19] M. Matsui, "The first experimental cryptanalysis of the Data Encryption Standard", in Annual International Cryptology Conference, pp. 1-11, August 1994. Springer Berlin Heidelberg.

[20] W. Diffie and M. E. Hellman, "Special feature exhaustive cryptanalysis of the NBS data encryption standard", *Computer*, vol. 10, no. 6, pp. 74-84, 1977.