Security Aware and Energy-Efficient Virtual Machine Consolidation in Cloud Computing Systems

Farhad Ahamed, Seyed Shahrestani, Bahman Javadi
School of Computing, Engineering and Mathematics
Western Sydney University
Sydney, Australia
17368113@student.westernsydney.edu.au, s.shahrestani@westernsydney.edu.au, b.javadi@westernsydney.edu.au

***Abstract*—The increasing number of data centers is consuming significant power with an upward surge. Hence, to preserve such huge energy and operating cost of data centers, the cloud service providers consolidate Virtual Machines (VM) to minimize the number of active physical machines. However, lack of reliable security measurements and policy enforcement during the consolidation process, have increased the security risks to the clients. In this paper, the compartment isolation technique is introduced to improve the system security during the consolidation process. The security-based selection and placement algorithms are also presented. The comparative analysis of this improved security approach shows that utilizing the proposed method will reduce the security risks without impacting the overall power consumption in data centers.**

Keywords— Cloud computing security; VM consolidation; VM security measurement; VM security

I. INTRODUCTION

Cloud computing is a heterogeneous architecture, on-demand self-service, broad network access and diversity of client devices, resource pooling, rapid elasticity, and measured service with the pay-per-use business model. Due to the advancement and availability of high-speed Internet, distributed and shared Cloud services have emerged leveraging the price. Hence, large numbers of data centres have outgrown to provision computing devices. The data centers have also added value to the customers by providing power and network redundancy, centralized management, reduced operating cost and physical security. Additionally, the advancement of virtualization technology has accelerated the resource sharing among the cloud servers, specifically, across the resources within the same data centers. A recent study shows that the cost of data center downtime has increased significantly for the companies in the last three years [1]. One of the main reasons for downtime is identified as cyber threat related to Distributed Denial of Service (DDoS). There is a novel approach in the data center marketplace to reduce the computing energy by the automatic consolidation of Virtual Machines (VM) into a minimum number of physical servers. Apparently, this would reduce the computing, operating and maintenance cost. However, there are obvious security risks to move across the VMs on a Physical Machine (PM), essentially, when there is no security policy supervised and provisioned and it is open to cyber-attack.

A rogue VM can be a potential entry point of a security breach within the shared PMs and in the wider network, despite the virtual network separation strategy within the data centres. Many of the attacks on Cloud systems relate to their distributed nature and shared resource environments. These attacks are considered as the traditional network threats that inherited to Cloud environments. Distributed Denial of Service (DDoS) attacks and Cross Site Scripting (CSS) threats are examples of this category. On the other hand, some threats are unique to Cloud environments. For instance, multi-tenancy nature of the Cloud server or VM forms the basis of the Cloud computing paradigm [2].

Construction of security profile is a novel idea which was proposed to improve the end user VM security during VM consolidation to reduce the operating costs in the data center [3]. A consolidated ranking based security profile can be created for the VMs in the data center that can be used for security aware VM consolidation. The compartment isolation method is proposed in this paper that is effective to reduce the security risks in a shared environment in the event of spreading of Malware. Also, security-aware energy efficient VM consolidation algorithms have been exploited with dynamic VM consolidation algorithms in this paper. A series of simulation results have been analysed which showed that the Secure Local Regression VM selection method with Minimum Migration Time (MMT) consolidation algorithm outweighs other secure dynamic algorithms at least by 5% measuring in the Energy times SLA violation (ESV). The solution presents an added protection measure with the minimal impact on energy efficient algorithm.

The rest of the paper is organized as follows. In section II, the background and motivation for this research are discussed. Next, in section III, the secure VM consolidation algorithms are presented. Consequently, in section IV, the experimental setup for the simulation is discussed in details. In section V, the simulation results are analysed and in section VI the concluding remarks and future work directions are presented.

II. BACKGROUND AND MOTIVATIONS

There are many cloud data centres in operation around the world to provide IT services for users. There are two major power related costs involve to run any data center. The first one of them is the cost of running the cooling system to ensure the server rooms are not overheated [4]. To provide energy to

the servers comprises the second major power cost in the data centre. The cloud providers apply VM consolidation policies to private, public or hybrid Cloud without exhausting security principles. There is a growing trend in the data centers to reduce energy cost. Hence, VM consolidation is introduced as an approach towards green Cloud computing to reduce the power consumption. However, co-residency of VMs can introduce some security challenges like the side-channel attacks and fate-sharing risks [5]

Multi-tenancy Cloud computing system is prone to disclosing CPU cache memory, timing analysis, and tracking of hardware resources. These can open the door to side channels that passively observe the information, or to covert channels that actively send data [6]. An attacker can detect the target VM in a server using the techniques like measuring cache usage, load-based co-residence detection and estimating traffic rates on network address [7]. When the virtual target instance and malicious instance are on the same PM, monitoring the CPU, memory, network utilization, and other behaviour patterns can lead to cross-VM information leakage.

On the other hand, some studies have indicated that the attacks on web services constitute more than 60% of the total attempts at exploiting online vulnerabilities [8]. It has also been shown that the injection flaws and cross-site scripting are among the most common liabilities of these services [9]. This is further complicated by noting that some of the provider sites, like Amazon, use Simple Object Access Protocol (SOAP) based Cloud control interface to monitor, add, and remove VM instances.

A botnet is a collection of compromised computers or bots. Botnets attackers may utilize Cloud resources to expand their network and processing power, posing a threat to the much-shared resources they are using on the same host [10]. DDoS attacks on the shared resources or on the Cloud server can cause devastating impacts in the provisioning of the Cloud services. Utility computing in Cloud environments is particularly vulnerable to such attacks, where the attackers seek to exploit the utility pricing model to harm the victim financially. It has also been shown that DoS attacks on Cloud systems can cause the OS kernel to crash and for some systems; the crash can be sustained at the VM level [11].

Considering the above-mentioned risks, it is essential to explore the methods which ensure the security of other tenants in the Cloud computing arena. One such method is to characterise a VM as unsafe or safe before actual VM consolidation. Then, During VM consolidation process the VM security profile can be utilized. In this paper, some algorithm has been proposed to improve the security during the VM consolidation process. Moreover, the expected outcome of the applied algorithm is presented. The outcome was reached after testing the solution in a simulated environment.

III. Security Aware Virtual Machine Consolidation

The VM consolidation technique allows migrating a VM from one PM to another PM based on some predefined rules and algorithms. The VM consolidation process often requires live migration of VMs. Live migration is a useful capability of virtualized clusters and data centres. It allows more exile management of available physical resources by making it possible to load balance and do infrastructure maintenance without entirely compromising the application availability and responsiveness.

Fig. 1 illustrates the simplified process of security aware VM consolidation. In a normal operation mode, the VMs reside in the same piece of PM. Each VM is provided with colour coded security measurements. When a secure VM consolidation process is executed, the VMs will re-arrange themselves and consolidate in a minimal number of PMs.

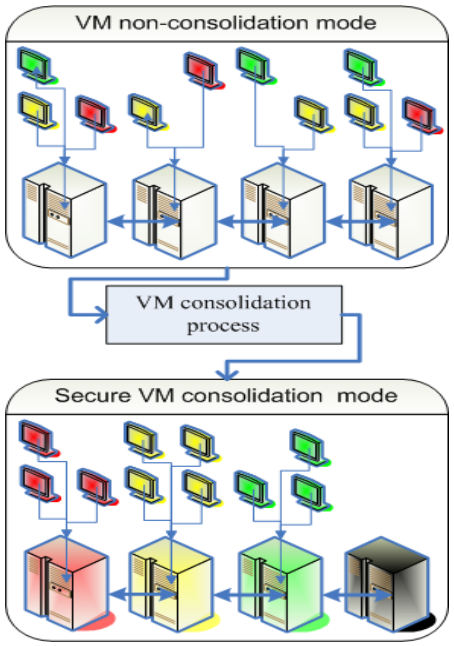

Fig. 1: Secure VM Consolidation Process

In the following sub-sections, the logical argument behind compartment isolation method presented, followed by the secure VM consolidation algorithms.

A. Compartment Isolation Method to Reduce Security Threat

Isolation and disinfection are an effective technique to improve network and system security. Isolation has been used in computing machines over the decades to protect valuable data and process. For example, programming languages use isolation method to determine which semantics, runtime systems or compilers will be allowed for a program execution without providing kernel level access to the remote program. A contemporary programming language like Java uses a certifying compiler which adheres to particular security policy during bytecode execution. There is a popular sandbox technique to provide the remote users limited execution environment. UNIX chroot jail is a sandbox method to provide remote users a virtual view of the file system. One of the most commonly used isolation is Operating System Kernel-based isolation. In this process, the OS-kernel layer is isolated with the application-layer. The Kernel level applications or the OS

has a higher priority and execution permission. The traditional monolithic kernels are examples of this isolation. There are other kernels focused on reducing Trusted Computing Base (TCB) instructions to remove the overhead of executing larger security policy. Microkernel, Exokernel, and Hypervisor are good examples of this. Isolation of the VMs based on the security profile is an effective way to improve the overall security of the Cloud computing platform.

"Fate sharing" is a concern in Cloud computing. It simply means, if one of the VM is quarantined or locked down due to illegal activity by the authority, the other VMs which are hosted on the same PM are inaccessible and locked down, sharing the same fate. Additionally, side-channel based monitoring and break-ins would be reduced if isolation is enforced. The third reason for isolation based security is to reduce chances of spreading malware or Botnet, which can utilise side-channel based method to infect the target host.

In order to improve the security while VM consolidation, in this paper, the Compartment Isolation method has been used. This method utilizes the SIR model technique. SIR model is well known in Computational Biology to analyse spreading and incubation of infection disease. SIR model is also studied in the relation to Computer virus, Malware, and Botnet [12]. In Fig. 2, the SIR model is shown where "S" represents the number of susceptible VMs being infected with particular Malware. "I" represents the total number of infected VMs which are actively trying to get access and spreading into other VMs. "R" represents a total number of recovered VMs.

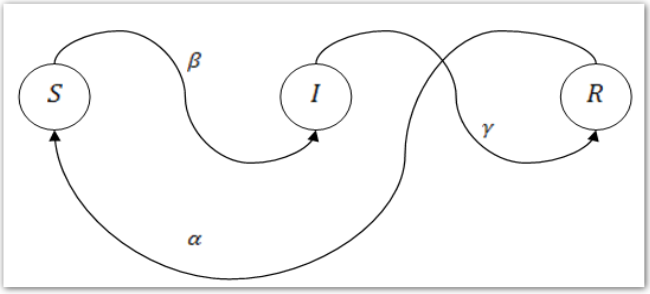

Fig. 2: SIR model

At any given time *t*, susceptible VMs is denoted as *S(t),* infected VMs denoted as *I(t)* and recovered VMs denoted as *R(t),* and the total number of VMs is N. According to the SIR model the relation is as follows:

$$S(t) + I(t) + R(t) = N(t) \quad (1)$$

According to the SIR model when *t=0,*

$$S(0) \approx N \quad (2)$$

The rate in which the VMs is turning to susceptible from recovery is α, the rate in which the VMs are getting infected from susceptible is β, and the in which the VMs are turning to recovery state from the infected state is γ. The dynamic model has the following relation according to the SIR model where S', I' and R' represents the dynamic number of the suspected, infected and recovered VMs, respectively. The relationships of this model are as follows:,

$$S' = \alpha R - \beta SI \quad (3)$$

$$I' = \beta SI - \gamma I \quad (4)$$

$$R' = \gamma I - \alpha R \quad (5)$$

According to the SIR model,

$$S' + I' + R' = 0 \quad (6)$$

When there is no VM infected, no possible Malware is spreading, therefore, $I' = 0$ is the virus-free equilibrium. Consequently, if $I' > 0$, which means there are infected VMs, there exists viral equilibrium.

There is a threshold quantity which determines whether an epidemic occurs or the Malware simply dies out. This amount is called the basic reproduction number, denoted by R_o. and can be defined as the number of secondary infections caused by a single infective introduced into a VM community made up entirely of susceptible individuals (S(0) ≈ N) over the course of the infection of this single infective. This infective individual makes β contacts per unit time producing new infections with a mean infectious period of 1/γ. Therefore, the basic reproduction number is when $I' = 0$ or there exist a virus-free equilibrium.

$$R_o = \frac{\beta}{\gamma} \quad (7)$$

This value quantifies the transmission potential of a virus. If the basic reproduction number falls below one (R_o < 1, i.e. the infective may not pass the infection on during the infectious period) the virus infection dies out. If R_o > 1, there is an epidemic in the Cloud. However, in cases where R_o = 1, the virus or malware becomes endemic, meaning the disease remains in the Cloud environment at a consistent rate, as one infected individual VM transmits the Malwares to one susceptible VM.

According to the SIR model, if isolated compartment strategy is introduced to isolate the infected VMs, the viral equilibrium changes. If there are a single malware and the probability of infection of a particular VM is *p,* the probability of all of the VMs infected is p^n. Consequently, if there are *m* numbers of Malware, the likelihood of infection of a VM with all malware is p^m and the probability of all the VMs infected by m number of malware is p^{nm}.

According to the SIR model when *t=0,*

$$S(0) \approx N$$

Therefore, all the VMs infected by *m* number of malware or probability of $S(0)$,

$$p(S) = p^{nm} \quad (8)$$

If there is *r* number of partitions, the probability of all the VMs infected by *m* number of malware will be

$$p(S/r) = \frac{p^{nm}}{r}, \qquad r > 1 \quad (9)$$

As,

$$p(S) > p(S/r) \quad (10)$$

It can be concluded from equation 10, using the isolated compartment strategy; separation of VMs will reduce the probability cross computer malware spreading. Therefore, a relatively less risk and remote environment can be created for the VMs with a secure VM consolidation process.

B. Secure VM Selection and Placement Algorithms

The following four items are required to be considered for combining and constructing a Security-aware VM consolidation method.

1. The host over-utilizing detection
2. The host under-utilizing detection
3. The VM selection method to identify the VMs for migration
4. The VM placement algorithm to determine the hosts to migrate to

The host is either over-utilized or under-utilized can be detected by observing its resources from VM management monitoring console. If the CPU upper threshold value is set to 90% and the lower threshold value is set to 10%, over-utilised and under-utilised VMs can be identified in the automated process.

When a host is detected as over-utilized or under-utilized, they are either selected to put a new VM in or take a VM out of that host. In this paper, the Security-Based Selection (SBS) is introduced. The SBS method considers the VM security profiles before selecting a VM to be a candidate for migration. If a PM is marked with the security level or threat level 10, the VMs which are already hosted on the physical host with the same ranking will stay. The other VMs will be a candidate to move out in the next migration cycle. There are also multiple selection methods to determine the VMs for migration [13].such as,

- Random selection (RS)
- Minimum migration time (MMT)
- Maximum co-relation (MC)
- Minimum utilisation (MU)

Before actual migration, a VM is selected based on some selection criteria to migrate to the appropriate PM. The SBS method that has been used in this paper selects the VMs to the next cycle of migration. In RS method, the VM migration candidates are randomly chosen to migrate to a PM.

Some of the popular and well-known VM placement algorithms are mentioned below. However, these are modified with Security-Based Placement (SBP) algorithm which is used in this paper:

- Local Regression (LR)
- Local Regression Robust (LRR)
- Median Absolute Deviation (MAD)
- Static Threshold (THR)

VM selection methods (RS, MMT, MC, MU) are altered to perform a security check to select a suitable VM. This selection formation is named as SBS that is mentioned earlier. Additionally, VM placement algorithms (LR, LRR, MAD, THR) are modified to perform a security check before actual placement of a VM into a PM. This procedure is named as SBP in this paper. Thus, the whole migration process ensures secure VM consolidation. The algorithm SBS and SBP algorithms are presented in Fig. 3 and Fig. 4, respectively.

```
Algorithm 1: Secure VM selection to migrate
Input host : Output vmToMigrate

migratableVMs <- getMigratableVMs(host)
minMetric <- MAX
foreach vm in migratableVMs do
    if vm is not in migration then
        metric = vm.getRam()
        if metric < minMetric  then
            if hostSecurityLevel != vmSecurityLevel
                vmToMigrate <- vm
return vmToMigrate
```

Fig. 3: Algorithm of security-aware VM selection

The input of the SBS algorithm is a physical host, and the output is a VM that is selected for migration. There could be many VMs available to migrate to that host. However, the SBS will filter out the most suitable VM for that PM. At first, all of the candidates VMs from a host are filtered out. By default, all the available VMs on that host should be considered in the first phase. One of the initial selection criteria for a VM is a larger memory. When a VM has a large memory, it will get a higher priority. Additionally, in the SBS process, if the VM and host security level do not match, the VM is selected for migration. In this method, the following two things are achieved.

1. Selecting a VM for isolation that is not compatible with the Host security level.
2. Selecting a VM that has a higher memory, thus reduces the migration time.

```
Algorithm 2: Secure VM placement
Input vmList, hostList Output

vmList.sortDecreasingUtilization()
foreach vm in vmList do
    minPower <- MAX
    allocatedHost <- NULL
    foreach host in hostList do
        if hostSecurityLevel Equals vmSecurityLevel then
            if host has enough resources for vm then
                power <- estimatedPower( vm, host)
                if (power < minPower) then
                    if( VMsInPM < AllowedMaxVM )
                        allocatedHost <- host
                        minPower <- power
    If allocatedHost !=NULL then
            allocation.add(allocatedHost, vm)
return allocation
```

Fig. 4: Algorithm of security-aware VM placement

When all the VMs are selected from the various hosts to migrate, the SBP algorithm starts. A migration map is prepared to process the actual migration. The migration map

table will keep the information related to the VMs and their designated PM for migration. In the SBP algorithm, initially, there will be a list of VMs that has been selected for migration. This list of VMs will be the input for the SBP algorithm. During the process of the algorithm, a PM is tested for a VM, if their security levels are matched, then it is checked that after the migration, the power utilisation should not reach to the MAX limit.

The estimatedPower() function checks the overall power consumption by the PM after the prospected migration. This value is compared with the MAX allowed power for each host in step 12 of Fig. 4 in the first iteration. With each loop, the lowest value of the minimal power utilisation is selected, and the security level is being checked. A high number of VMs in a PM can impact the performance. Therefore, a variable VM_PER_PM will be used throughout the VM migration process to enforce a limit on the maximum number of VMs per PM. A qualified VM will be added to a VM allocation table that will be assigned to a PM. When the allocation table is constructed, the simulation core will allocate the VMs to the designated PMs. Thus, a single migration step will be complete. Throughout the process, this migration cycle will run continuously. A variable SCHEDULING_INTERVAL is used to control the frequency of migration cycle.

IV. SIMULATION SETUP FOR EVALUATION

In order to evaluate the proposed algorithms, we used CloudSim simulator. CloudSim is an open source, extensible and programmable simulator. It is also a flexible simulation tool to simulate a cloud computing environment [14]. It can be used to consolidate the VMs based on the security profile. CloudSim can generate a large-scale of VM testing environments. It provides multiple tools and mechanism to create a data center with the resources.

The experimental setups were done to get the results for three different types of simulation scenarios. In these simulations, several types of workload have been applied to evaluate the impact of secure VM consolidation. One of the simulation scenarios is based on incremental workload over a period of time, which classified as low to medium grade workload. Scalability of the solution also has been checked by changing the number of Cloud resources. The sections *A, B* and *C,* describe various simulation scenarios in which the simulation study was conducted.

A. Setup to Evaluate on Low-Medium Workload

A sample workload data has been used from PlanetLab to study and evaluate the impacts of the secure VM consolidation on low-medium workload. Real world lower-medium workload data from PlanetLab has been collected for ten random days [15]. The average workload of the randomly collected sample varied from 5%-30%. These workloads have 288 data collection points of CPU utilization for a given VM for any given day. Therefore, each data point represents CPU utilization value of every 5 minutes interval. A power consumption table was formed to compare the host utilization with the power usage by the host. For example, the power profile Table I exhibits a modest correlation between CPU utilization and power consumption. In one of the simulation low-medium workload and "end server", power profiles are used based on the SPEC definition [16]. This relation between CPU utilization and power consumption of the server is coded into the simulation tool.

TABLE I. SERVER POWER CONSUMPTION PROFILE BASED ON UTILIZATION

Server load	***HP ProLiant G4(W)***	***HP ProLiant G5(W)***
0%	86	93.7
10%	89.4	97
20%	92.6	101
30%	96	105
40%	99.5	110
50%	102	116
60%	106	121
70%	108	125
80%	112	129
90%	114	133
100%	117	135

Two types of server power models are taken into consideration in this simulation scenario. The First one is HP ProLiant G4 and the second one is HP ProLiant G5. According to the statistical data of Table I, power consumption increases by 27% when CPU utilization jumps from 0% to 100%.

TABLE II. VM AND PM INITIAL CONFIGURATION FOR SIMULATION

Virtual Machine Details	
Total MIPS of VM	2500
Total PES (Processor unit) of VM	1
Total RAM of VM	1024 MB
Network Bandwidth of VM	100 Mbit/s
Total Storage size of VM	2.5 GB
Physical Machine Details	
Total MIPS of PM	2660
Total PES (Processor unit) of PM	2
Total RAM of PM	8192 MB
Total Storage size of PM	80 GB

The specifications of VM and PM also are shown in Table II for this simulation scenario to observe the impact of security aware VM consolidation when the workload is low-medium.

There had been multiple levels of isolation based on their dynamic security profile. Each level was used to isolate the VMs. In the simulated data center, there were 800 physical

hosts and 1052 VMs. Migration cycle was set to every 1 hour, which means VM overload detection and VM consolidation will kick in every hour. The simulation was set to run with the available workload information of a day (20110303) from the PlanetLab workload samples.

B. Setup to Evaluate Scalability of the Solution

In this simulation scenario, the host numbers were scaled to verify and observe the performance of the solution. The hosts' numbers were increased by 2 to 3 times. The following variables were used to configure new test environment,

VM_TYPES = 4 (Types of VM)

HOST_TYPES = 2 (Types of Server)

VM_PER_PM = 100 (Max allowed VM in a PM)

INITIAL_SECURITY = true (VMs and PMs will be marked with a security tag during initialization)

RANDOM_SECURITY_PROFILE = true (Security profiles will be created randomly)

SCHEDULING_INTERVAL = 300.0 seconds (Frequency of Migration)

SIMULATION_LIMIT = 86400.0 seconds (Max simulation run time)

NUMBER_OF_HOSTS = 1000 (Max available host in a data center)

C. Initial Setup to Evaluate SLA and Energy Utilisation

Security policy was applied to multiple VM consolidation algorithms available in CloudSim to identify the best optimal algorithm while considering the consumption of energy. One of the random workload instances 20110303 was selected for this particular evaluation. According to the workload characteristic, there are more than 1000 VMs which will be deployed on 800 PMs in the simulator. For simplicity, VM migration cycle was set to 1 hour, which means there was 24 cycles of VM migration in that particular simulation. Maximum 8 VMs were allowed to run in a single PM, considering the VM and PM sizing as below. Every VM and PM had the characteristics shown in Table II earlier.

V. RESULTS AND DISCUSSIONS

In this section, the output of the simulations for various scenarios and working conditions are presented.

A. Results for Low-Medium Workload

The outcome of the simulation is plotted in Fig. 5. The Y-axis represents energy in kWh hours, and the X-axis represents the degree of isolation based on security. From the graph, it can be observed that there is a gradual power increment when the level of security is being increased. When the security level was incremented from 2 to 10, the power consumption rose 1.8 %.

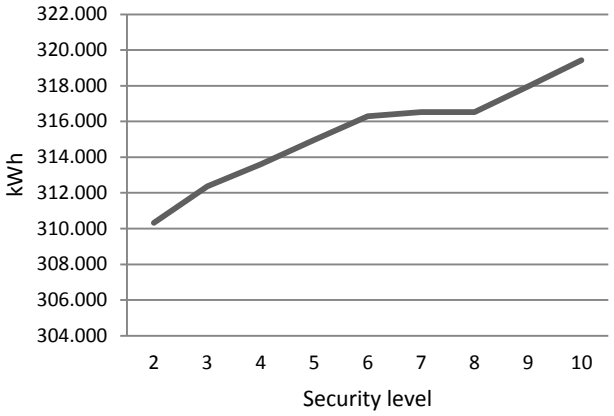

Fig. 5: Security aware VM consolidation comparison for low-medium workload for 800 hosts.

It can be observed that when the security level was in between 6 to 8; the curve is parallel to X-axis which indicated that the same number of PM was running to serve the VMs during those VM isolations.

B. Scalability of Security Aware VM Consolidation

Fig. 6 shows the energy versus security graph when the data centre has 1000, 2000 and 3000 PMs. It has been observed that when there was no security policy (level 1) comparable to when there were 7 security levels, the energy consumption was a little bit higher. However, there is no significant difference after applying the security policy in VM consolidation.

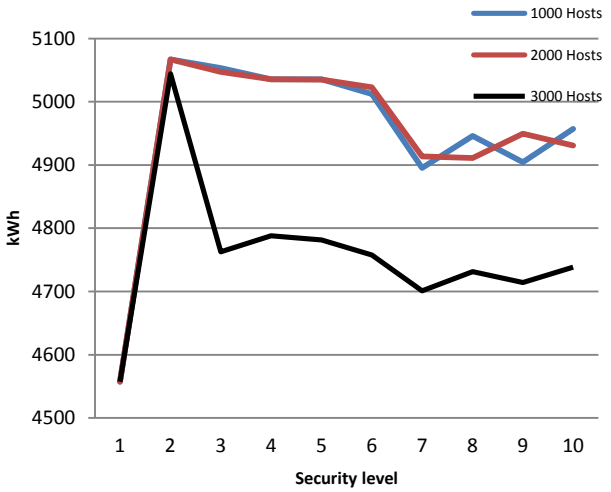

Fig. 6: Energy consumption versus security graph when the number of PMs are 1000, 2000 and 3000.

Initially, when there was no security policy in the algorithm (level 1) compare to security-aware VM consolidation (>= level 2), the power consumption jumped by 11% as an average for all these 3 scenarios. However, when

the security level is increased, the kWh does not change abruptly.

Fig. 6 also shows the results of the power consumption and security trade-off when there are 1000 to 3000 hosts in a data center. It is evident from the graph that the primary energy consumption was lower when there was no security policy (level 1). When the isolation occurred to second degree, there is a spike in the consumed energy. However, in the long run, this energy vs. security graphs demonstrates that when the isolation or level of security is increased, the energy the consumption stabilises although the consumption level stays above the level 1. It can be noticed that when the hosts were increased to 3000, the energy consumption level was lower than the other two scenarios. It means fewer numbers of PMs were actually needed to maintain compartment isolation. On the other hand, when 1000 or 2000 hosts were used to run the same workload, it required more PMs to maintain compartment isolation.

Therefore, after careful observation of the graphs, it can be concluded that the graphs represent consistent behaviour on energy consumption; either the data centre size is compact or oversized. Moreover, it can be concluded that the solution is scalable and works with a higher number of Cloud resources without any bottleneck.

C. Impact on SLA and Power Utilisation

There are several VM selections and placement algorithm that can be used as a VM consolidation pair to implement the security-aware VM consolidation. Each VM consolidation algorithm was checked after applying the security policy-based isolation. Fig. 7 shows that when the security level is increasing, the power consumption is also growing at a moderate pace. When the security level is increased from two to ten, the energy consumption is increased by 3% as an average for all the algorithms.

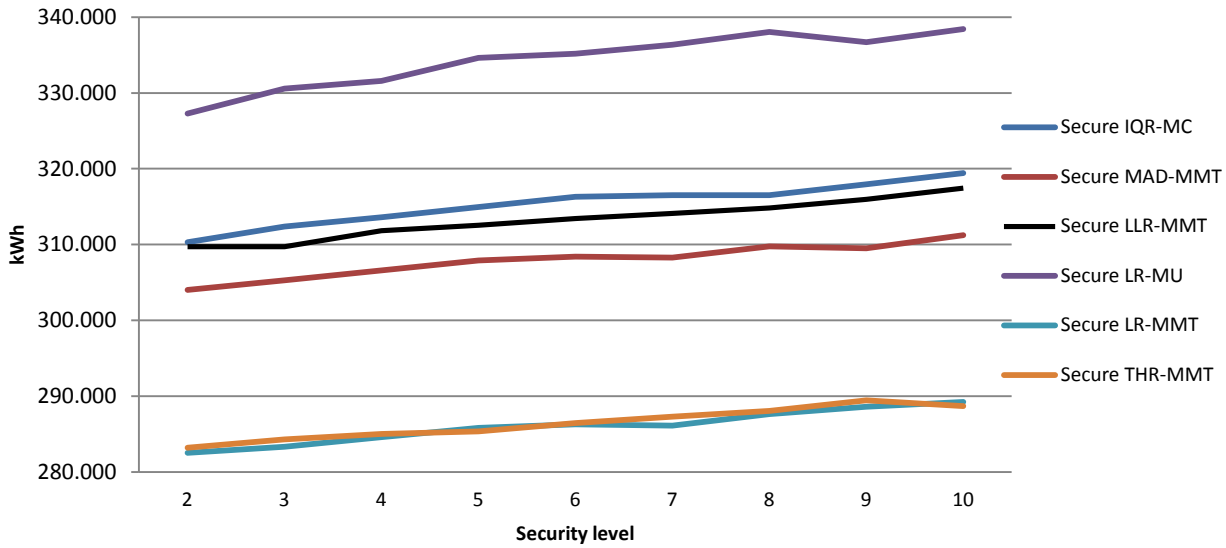

Fig. 7: Security level vs. energy consumption in multiple security-aware algorithms

In the Secure MAD-MMT combination, when the security level is increased from two to ten, the energy consumption rate is increased by 1.5%. In Secure LLR-MMT combination when the security level is increased from two to ten, the energy consumption is increased by 1.2%. Similarly, it can be observed, in Secure LR-MU combination when the security level is increased from two to ten; the energy consumption is increased by 2.5%. In Fig. 7, the bottom two curves demonstrate lower energy consumptions. One of them labelled as Secure THR-MMT, and the other is Secure LR-MMT. The output of these two algorithms gives close proximity of being the best performing algorithm. In Secure LR-MMT combination when the security level is increased from two to ten and the energy consumption is increased by 1.8%. In Secure THR-MMT combination, when the security level is increased from two to ten, the energy consumption is increased by 1.7%.

The common features of Fig. 7 are as follows,

- An increased security level results in increased energy consumption in general.
- The Secure LR-MMT provides the best economic security solution as compared to the other peer security-aware VM consolidation (according to Table III).

TABLE III. SECURITY AWARE VM CONSOLIDATION VS. ESV

Secure VM Algorithms	*kWh*	*Avg SLA violation*	*ESV*
Non-power aware	2484	0	0
DVFS	1046	0	0
IQR MC	315.33	10.09	3181.68
MAD MMT	307.88	10.09	3106.509
LR MU	334.31	10.08	3369.845
LR MMT	286.02	9.71	2777.254
THR MMT	286.42	10.24	2932.941

In Table III, it can be observed that Secure LR-MMT has the lowest average of SLA violation as well as lowest ESV. The bottom ESV value determines the best VM migration policy according to Beloglazov and Buyya [13] . Therefore, security aware LR MMT is clearly outweighed other algorithms.

VI. CONCLUSIONS

In this paper, we have introduced the compartment isolation technique to achieve the security aware VM consolidation. We have implemented the proposed SBS and SBP algorithms in CloudSim and analysed the behaviour of the Cloud resources in a controlled environment. Different types of simulation setup and the subsequent result confirms that there are no abrupt changes in power consumption to achieve security aware VM consolidation. Various workloads and computing resources have been tested to reach into this finding. The solution presents itself as scalable that has been tested with the simulator. It has been observed, security aware energy efficient VM consolidation algorithm that exploits dynamic VM consolidation algorithms demonstrate similar characteristics compare to non-security aware VM consolidation. LR version of the SBS VM selection method with MMT version of the SBP consolidation algorithm outweighs other SBS and SBP based dynamic algorithms at least by 5% measuring in the ESV. The solution presents an added protection measure with the minimal impact on energy efficient algorithm. The solution is scalable in terms of processing concentration. For example, If VMs are concentrated 19 times higher than the default capacity, secure consolidation could reduce energy waste by 27%. The solution exhibits consistency throughout low and a high degree of the workload in a data centre. This work could be extended to improve the VM reliability as well as security and energy consumption.

REFERENCES

[1] E. N. Power, "Cost of Data Center Outages," presented at the Data Center Performance Benchmark Series, 2016.

[2] Y. Chen, V. Paxson, and R. H. Katz, "What's new about Cloud Computing Security? ," *EECS Department, University of California, Berkeley,* 2010.

[3] Ahamed. F., Shahrestani, S. and Javadi, B. (2015). Developing Security Profile for Virtual Machines to Ensure Secured Consolidation: Conceptual Model. In Proc. 13th Australasian Symposium on Parallel and Distributed Computing (AusPDC 2015) Sydney, Australia. CRPIT, **163**. Javadi, B. and Garg, S.K. Eds., ACS. 85-91.

[4] E. Pakbaznia and M. Pedram, "Minimizing data center cooling and server power costs," in *Proceedings of the 2009 ACM/IEEE international symposium on Low power electronics and design*, 2009, pp. 145-150.

[5] J. Shi, X. Song, H. Chen, and B. Zang, "Limiting cache-based side-channel in multi-tenant cloud using dynamic page coloring," in *Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on*, 2011, pp. 194-199.

[6] Y. Xu, M. Bailey, F. Jahanian, K. Joshi, M. Hiltunen, and R. Schlichting, "An exploration of L2 cache covert channels in virtualized environments," presented at the Proceedings of the 3rd ACM workshop on Cloud computing security workshop, Chicago, Illinois, USA, 2011.

[7] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," presented at the Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2009.

[8] SANS Institute. (2009). *The top cyber security risks* [Webpage]. Available: http://www.sans.org/top-cyber-security-risks

[9] Open Web Application Security Project. (2010). *OWASP Top 10 Risks* [Webpage]. Available: http://www.owasp.org/index.php/Top_10_2010

[10] S. Kandula, D. Katabi, M. Jacob, and A. Berger, "Botz-4-sale: surviving organized DDoS attacks that mimic flash crowds," presented at the Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation - Volume 2, 2005.

[11] A. Kurmus, M. Gupta, R. Pletka, C. Cachin, and R. Haas, "A comparison of secure multi-tenancy architectures for filesystem storage clouds," presented at the Proceedings of the 12th ACM/IFIP/USENIX international conference on Middleware, Lisbon, Portugal, 2011.

[12] M. Peng, X. He, J. Huang, and T. Dong, "Modeling Computer Virus and Its Dynamics," *Mathematical Problems in Engineering,* vol. 2013, p. 5, 2013.

[13] A. Beloglazov and R. Buyya, "Optimal online deterministic algorithms and adaptive heuristics for energy and performance efficient dynamic consolidation of virtual machines in Cloud data centers," *Concurrency and Computation: Practice and Experience (CCPE),* vol. 24, pp. 1397-1420, 2012.

[14] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. De Rose, and R. Buyya, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," *Software: Practice and Experience,* vol. 41, pp. 23-50, 2011.

[15] K. Park and V. S. Pai, "CoMon: a mostly-scalable monitoring system for PlanetLab," *ACM SIGOPS Operating Systems Review,* vol. 40, pp. 65-74, 2006.

[16] S. Benchmarks, "Standard performance evaluation corporation," ed, 2011.