Migration of Virtual Machine to improve the Security in Cloud Computing

N. Chandrakala, B. Thirumala Rao
Dept. of CSE, K L University, Guntur, AP, India

Article Info

Article history:

Received Jan 19, 2017
Revised Aug 25, 2017
Accepted Sep 14, 2017

Keyword:

Cloud computing
Cloud Security
DTMC
Migration of VM
Survivability

ABSTRACT

Cloud services help individuals and organization to use data that are managed by third parties or another person at remote locations. With the increase in the development of cloud computing environment, the security has become the major concern that has been raised more consistently in order to move data and applications to the cloud as individuals do not trust the third party cloud computing providers with their private and most sensitive data and information. This paper presents, the migration of virtual machine to improve the security in cloud computing. Virtual machine (VM) is an emulation of a particular computer system. In cloud computing, virtual machine migration is a useful tool for migrating operating system instances across multiple physical machines. It is used to load balancing, fault management, low-level system maintenance and reduce energy consumption. Virtual machine (VM) migration is a powerful management technique that gives data center operators the ability to adapt the placement of VMs in order to better satisfy performance objectives, improve resource utilization and communication locality, achieve fault tolerance, reduce energy consumption, and facilitate system maintenance activities. In the migration based security approach, proposed the placement of VMs can make enormous difference in terms of security levels. On the bases of survivability analysis of VMs and Discrete Time Markov Chain (DTMC) analysis, we design an algorithm that generates a secure placement arrangement that the guest VMs can moves before succeeds the attack.

Corresponding Author:

N. Chandrakala,
Dpt of Computer Science and Engineering,
K L University,
Guntur, AP, India.
Email: kala5136@gmail.com

1. INTRODUCTION

In current public cloud, VMs are installed in the same physical machines. Some of VMs working in the same subnet or physical server may collaborate in order to complete a service. Collaborating with vulnerable VMs or running in the physical server with malicious VMs will increase the security risk. The connections between VMs via network or shared physical resources will introduce attacks. The external adversary can compromise a vulnerable VM, then find next target via network connection. Also he can deploy a malicious VM and attack other VMs in the same physical server. In order to improve the security of the entire cloud, we design a VM placement strategy which will migrate the legitimate VMs to a secure physical servers or network. Cloud placement policies allow virtual machines created in a virtual data center to be placed on resources with matching policies. With the increase in the popularity of cloud computing systems, virtual machine migrations across data centers and resource pools will be greatly beneficial to data center administrators. Cloud computing is rapidly attractive more and more vital in computing infrastructures. An example of virtual machines placement strategy is shown in Figure 1. Each VM on every node (physical server) may execute different services and some of VMs are dependent on others. Node is a physical machine where runs a few of VMs with the limit of hardware resources. The cloud provider is the owner of a public cloud and sells the cloud resources to cloud users. The cloud provider also takes charges of managing the cloud resources and protecting users' privacy. Therefore, cloud provider will design and deploy VMs placement strategy in a public cloud.

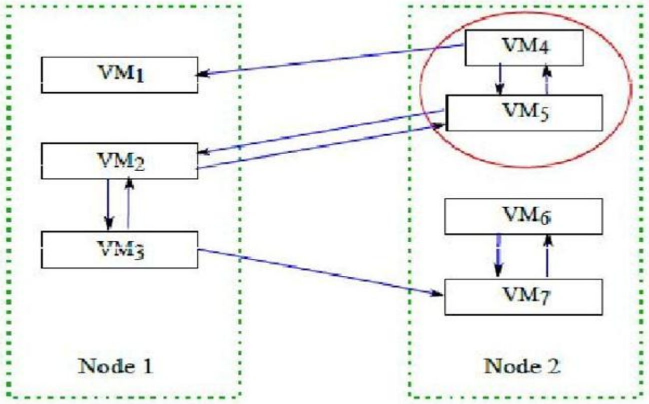


Figure 1. Virtual machines placement strategy example

Cloud computing distributes the computing tasks to the resource pool made from a large number of computers. VMs refer to one instance of an operating system along with one or more applications running in an isolated partition within the computer. There will be multiple virtual machines running on top of a single physical machine. When one physical host gets overloaded, it may be required to dynamically transfer certain amount of its load to another machine with minimal interruption to the users. This process of moving a virtual machine from one physical host to another is termed as migration. In the past, to move a VM between two physical hosts, it was necessary to shut down the VM, allocate the needed resources to the new physical host, move the VM files and start the VM in the new host. The live migration makes possible for VMs to be migrated without considerable downtime. The transfer of a VM actually refers to the transfer of its state. This includes its memory, internal state of the devices and that of the virtual CPU. Among these, the most Time-consuming one is the memory transfer.

We have already found many attacks against vulnerabilities in cloud hypervisor and the control VM. For example, some adversaries exploit the vulnerabilities of cloud hypervisor (e.g. CVE-2007-4993, 2007).Once they compromise the hypervisor (e.g. KVM and Xen), the users' VMs will be taken over. Some other attackers will place a malicious VM in the public cloud and compromise the VMs running in the same physical server by side channel attack [1]. Additionally, the adversary can find the next target by analyzing the network connections of compromised VMs.

2. RELATED WORK

In IT industry, different computing needs are provided as a service. There are many benefits of using the technology available from cloud service providers, such as access to large-scale, on-demand, flexible computing infrastructures. However, increasing the dependability of cloud computing is important in order for its potential to be realized. Data security is one of the most critical aspects in a cloud computing environment due to the sensitivity and importance of the information stored in the cloud, as is the trustworthiness of the cloud service provider. The risk of malicious insiders in the cloud and the failure of cloud services have received intense attention by cloud users [2]. The cloud computing provides an opportunity of development and environment for new service pattern of multi-source information service (MSIS). The issues associated with cloud computing and the nature part of the relation between MSIS and cloud computing [3]. Cloud computing offers distributed and shared computing resources and services that belong to different service providers and websites. One of the most important aspects that need special attention pertains to the cloud security. Cloud computing has the important component as trust management [4]. The major issues pertaining to data security in the cloud computing environment like data location and data transmission, data availability, data security are discussed in [5]. Behl [6] explores cloud computing security issues and highlights the key research challenges that include: availability and performance, malicious insiders, outside attacks, service disruptions.

Chen et al. [7] discuss cloud computing data security and data privacy protection issues. The security architecture is defined at three levels: software security, platform security, and infrastructure security. Data privacy protection issues of the data lifecycle in cloud computing include transfer, use, share, storage, archival and destruction. Popovic et al. [8] indicate security issues of cloud computing systems by highlighting the problems of cloud computing, particularly, the security management models based on security standards and the security issues pertaining to security standards. Siani et al. [9] highlight that the major hurdles in large-scale acceptance of cloud computing, mostly due to service security and privacy issues. Based on the discussed scenarios, it is recommended that sensitive information should be minimized when data is processed on cloud and privacy to the end-user must be assured.

As the number of dependents on the cloud services shoots up, the security issue has become an overwhelming problem for cloud service providers. In order to make use of the cloud benefits to full extent, these issues need to be addressed first. The major security issues in cloud computing and some of the countermeasures that can be implemented are also suggested in [10]. Dawei Sun et al. [11] has classified the security issues into six categories. The need for monitoring the cloud server, data confidentiality, malicious insiders activities, service hijacking, issues due to multi tenancy and so on are dealt with. Privacy issues like enabling users to have control over data, preventing data loss while replicating etc are also discussed. D. Zissis, D. Lekkas [12] has addressed various security issues like trust, confidentiality and privacy, integrity and availability. In a cloud environment trustworthiness is a relevant term as data is outsourced out of owner‟s security boundaries.

John C. Roberts II and Wasim Al-Hamdani [13] has discussed about "wrapper attack" in which the attacker wraps some malicious code in XML signature and injects this signature into the XML codes which is essential in cloud computing for resource sharing. Cloud computing has become a tempting target for cyber crime [14]. The prominent providers like Amazon and Google has mechanisms to defend against this type of attack. A cloud environment consists of numerous heterogeneous entities and the security of such an environment is dependant of the security guaranteed by the weakest entity. Various security issues [15] in the different delivery models of cloud threaten the end-users. In Software as a Service (SaaS) model they have quoted various issues like data confidentiality, web application security, data breaches, virtualization vulnerability, availability, backup, Identity management and sign-on process. The management of information security operations is a complex task, especially in a cloud environment.

The cloud service layers and multi-tenancy virtual architecture create a complex environment in which to develop and manage an information security incident management and compliance program. The goal is to protect cloud services against new and existing attacks as well as comply with security policies and regulatory requirements. The proposed approach provides better managed services for customers wanting to outsource their information security operations to attain reliable, transparent, and efficient cloud security and privacy [16]. Cloud computing promises to increase the velocity with which application are deployed, increase innovation and lower costs. Cloud computing incorporates virtualization, on demand deployment, internet delivery of services and open source software. From another perspective, everything is new because cloud computing changes how we invent, develop, deploy, scale, update, maintain and pay for application and the infrastructure on which they run. Because of these benefits of cloud computing, it requires an effective and flexible dynamic security scheme to ensure the correctness of users' data in the cloud. Quality of service is an important aspect and hence, extensive cloud data security and performance is required [17].

3. PROPOSED WORK

In order to protect user's privacy in public cloud, we propose a migration based approach which generates the VM placements strategy based on security evaluation of each VM. To evaluate the security of each VM, we deploy Discrete Time Markov Chain (DTMC) and predict the possibility of each VM being compromised. Then a placement strategy will be produced based on security evaluation. After VMs migration, users' VMs will survive before the attack completes. Meanwhile, our approach also considers the performance overhead because the closer connected VMs are placed, the better performance the cloud platform will acquire. To the best of our knowledge, this approach is the first effort to develop the following mechanisms and techniques to enhance cloud security through changing cloud placement. The contribution of my migration-based placement strategy is as below:

1. We present a systematic approach to predict the possibility of VM on each attack step, and then move away the VMs before attack succeeds.
2. We propose an algorithm to generate a secure placement plan which also takes performance cost into consideration.

3. The evaluation results in a real public cloud show my approach can greatly improve the security of entire cloud platform.

In order to accurately estimate the current network security situation an awareness and analysis method for network real-time threats is proposed. This method recognizes current real-time threats and predicts subsequent threats by modeling attack scenario. The threat awareness model is constructed with expanded finite-state automata, which is defined as attack state transition graph and is shown in Figure 2. Based on the former all possible intruding paths and state transformation can be illustrated, and based on the latter really happening threats and intruding path are described. Then a threat awareness algorithm is presented based on the above model. With this algorithm, various kinds of invalid threats are filtered; current valid threats are obtained by correlating dynamic alarms with static attack scenario.

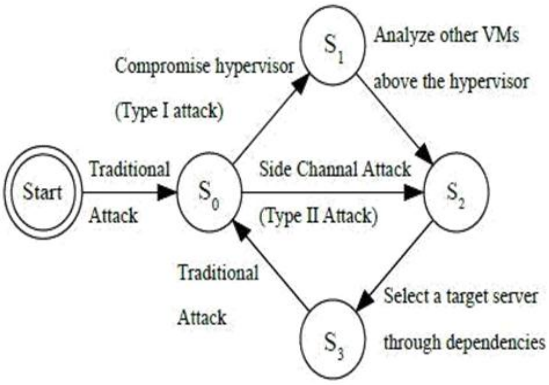


Figure 2. Attacks state transition graph

Generally, the adversaries should take several steps to compromise a VM. As shown in attacks state transition graph (Figure 2), the adversary starts from compromising one VM on a new server (S_0). After hypervisor is compromised (S_1), the adversary will collect dependency information of compromised VMs (S_2). Finally, new target server will be selected (S_3).We make the following assumptions on cloud adversaries who want to compromise the VMs and users privacy.

1. The cloud adversaries can detect the vulnerabilities of both cloud platform and virtual machines.
2. The cloud adversaries will follow the attack transition graph to compromise a VM step by step.
3. The cloud adversaries always choose the easiest target in term of the vulnerabilities.
4. The attacker has no view of the cloud view at the beginning of the attacks. However, the attacker may acquire more knowledge after compromising more nodes in the cloud.

If the cloud provider can migrate VMs to a safe node before the node is compromised, migrated VMs will survive this attack. We set up the following goals when design the placement algorithm.

1. Reduce the number of compromised VMs.
2. Increase the survivability of services.
3. The placement algorithm is also compatible with performance requirements.

In order to verify the improvement of survivability after migration, we define the survivability of a service in Theorem 1.Then we need to evaluate the survivability of a node as shown in Theorem 2.

Theorem 1: Survivability of a Service

Given a service S_i (VM chain) including some related Si = {VM_a, VM_b,……., VM_n} and
node set N = {N_1, N_2, …, N_m},

If the survivability in specific attack step for the Nodes which hold the VM belong to
S_i = {PN_1, PN_2, …., PN_m}, Then,

Survivability (PS) for service S_i is below:

$$PS_i = \prod_{j=1}^{m} PN_j. \quad (1)$$

Theorem 2: Survivability of a Node

Given a node N and a set of VM_s={VM_a, VM_b,……., VM_n}

which locate at node N, and the compromised probability for these VMs are {P_a, P_b, …., P_m}, the survivability (PN) for Node N is below:

$$PN_N = \prod_{j=1}^{m}(1 - P_j) \tag{2}$$

4. CLOUD MIGRATION BASED ARCHITECTURE

Developing a cloud migration strategy requires understanding beyond what's in the vendor brochures. You need to understand the architecture of that environment. You need to understand the potential risks and the potential harm to your organization from exposing it to those risks. That influences your ability to properly assess a given cloud and it empowers you to form criteria and then determine what type of cloud environment your organization needs and again to what extent you should be adopting cloud-based IT resources. The structure of migration-based approach is shown in Figure 3. In order to accomplish the design goal, my approach includes three components: security evaluation, strategy generation, and performance evaluation. First of all, the dependency exploration mechanism detects the service dependencies among VMs through network connections. We evaluate each VM’s security level according to the vulnerabilities found in VM’s operating system. Afterwards, we utilize DTMC to expect the possibility of successful attacks in each attack step. Finally, we design an algorithm to create the placement plan which takes security and performance into consideration.

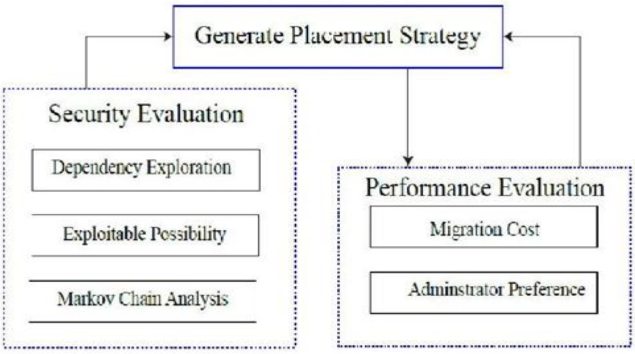


Figure 3. Cloud migration based architecture

There are three common categories for approaching cloud migration: Machine to machine, application migrations, and DevOps driven migrations. In all three categories you can move everything, or you can focus on moving certain workloads and take a hybrid approach. Selecting the workloads to move may be based on refresh cycles, new projects or to gain experience and confidence in a **cloud-based architecture**. Let’s start with the simplest strategy: machine to machine migrations. Machine to machine migration involves moving virtual machines or physical servers from one environment into the target cloud environment. While this form of migration is the simplest from an architectural perspective, it also provides the least benefit, with only some operational efficiencies able to be realized. This lift and shift approach is usually chosen when a business has no other options or has a requirement for a more rapid migration.

The second common type of migration is application migration. This involves building fresh infrastructure in the cloud such as servers, storage and networking, then installing the legacy applications, followed by a data migration exercise. The notable benefit compared to a lift and shift approach is that it allows for re-architecture, while providing better operational efficiencies. Compared to a lift and shift migration, there is a higher degree of risk involved, however this is something that can be addressed with appropriate planning and discovery.

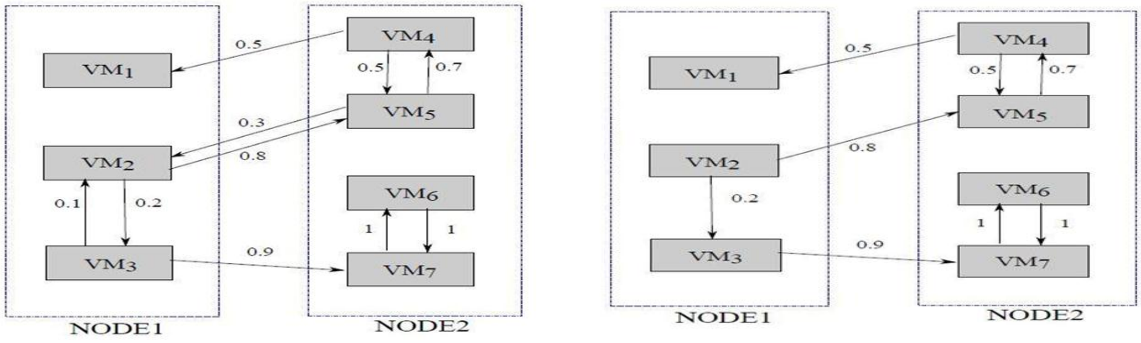
The third and final type of migration we’re looking at is a DevOps driven migration. A DevOps driven Migration is one that provides maximum agility and quality and will also provide long-term benefits for your business. Hallmarks of a DevOps driven migration are the capability to have Continuous integration (CI) and continuous delivery (CD), allowing you to fix bugs and provide new features sooner. It also provides an opportunity to re-align technology to the business requirements of the organization. A DevOps driven migration ensures greater visibility and control over the release process and increased scope for collaboration across your development and operations team. One of the most commonly cited reasons for a DevOps driven migration is increasing agility for the business, enabling innovation and the ability to change direction quicker and easier. Picking the right cloud migration approach for your business means analyzing what are the business requirements, goals, current pain points and what do you want to get out of your infrastructure. Careful consideration of these factors, coupled with planning and discovery can help a business maximise their investment in the cloud and begin realizing the benefits sooner.

5. EXPERIMENTAL RESULTS ANALYSIS

In order to quantify the vulnerability, we firstly scan the guest VMs and detect the vulnerabilities matched in national vulnerability database (NVD). Afterwards, discrete time Markova chain analysis (DTMC) will predict the possibility of successful attacks in each step. Common vulnerability scoring system (CVSS) provides a framework to scan the guest VM and score security of guest VMs based on vulnerabilities. There are three metrics group in CVSS system: base, temporal, and environment. Each of them can represent different characters of vulnerabilities.

5.1. Markov Chain Analysis

In order to represent the attack path and possibility of successful attack in each step, we will use attack dependency graph (ADG) based on Markov chain Analysis as shown in Figure 4. The procedure of DTMC prediction is explained as follows:



(a) Step 1 (b) Step 2

Figure 4. Attack dependency graph based on Markov chain analysis

For *n* nodes in ADG graph, assume the initial probability distribution on each node is,

$$\underline{\pi}(0) = (1, \underbrace{0, 0, \ldots, 0}_{n-1})$$

1. The initial $\underline{\pi}(0)$ is determined by attacker's first choice.
2. In attack step 1, the possibility distribution of attacker can compromise connected VM's is,

$$\underline{\pi}(1) = \underline{\pi}(0)P^1$$

3. After k^{th} step attack, the possibility distribution will become,

$$\underline{\pi}(n) = \underline{\pi}(0)P^n$$

Where

P is the state-transition probability matrix of DTMC and

$$\mathbb{P} = \underbrace{\mathbb{P} \cdot \mathbb{P} \cdots \mathbb{P}}_{n}$$

For example, Figure 4(b): step 2 is used as an example to explain how DTMC predict the attack possibility in each step. I assume that the first compromised VM should be VM_2,

Hence,

$$\underline{\pi}(0) = \{0\ 1\ 0\ 0\ 0\ 0\ 0\}$$

Hence we may obtain the attack possibility from above assumption. For example, the edge from VM_3 to VM_7 is 0.9, which indicates that after VM_3 is compromised, VM_7 will have 90% chances to be taken over by the attacker.

The corresponding state-transition probability matrix P is as follows.

$$\mathbb{P} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.2 & 0 & 0.8 & 0 & 0 \\ 0 & 0.1 & 0 & 0 & 0 & 0 & 0.9 \\ 0.5 & 0 & 0 & 0 & 0.5 & 0 & 0 \\ 0 & 0.3 & 0 & 0.7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{3}$$

For Step 1, we get the possibility of being compromised for each VM is,

$$\pi(1) - \{0\ 0\ 0.2\ 0\ 0.8\ 0\ 0\}$$

Based on the result, VM_5 is the most dangerous VM, and then we remove the edges which point to VM_5 because the attacker will not compromise VM_5 again in the following attack path.

Hence, the result of matrix $\mathbb{P}'$ after step one should be as follows and the DAG should be:

$$\mathbb{P} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0.1 & 0 & 0 & 0 & 0 & 0.9 \\ 0.5 & 0 & 0 & 0 & 0.5 & 0 & 0 \\ 0 & 0.3 & 0 & 0.7 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{4}$$

Markov chain analysis will end if the step reaches the longest path in an ADG.

Hence, the probability distribution for the initial state and the first 6 steps are as follows.

$$\begin{pmatrix} \underline{\pi}(0) \\ \underline{\pi}(1) \\ \underline{\pi}(2) \\ \underline{\pi}(3) \\ \underline{\pi}(4) \\ \underline{\pi}(5) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0.2 & 0 & 0 & 0.8 & 0 \\ 0 & 0.26 & 0 & 0.56 & 0 & 0 & 0.18 \\ 0.56 & 0 & 0.26 & 0 & 0 & 0.18 & 0 \\ 0 & 0.026 & 0 & 0 & 0 & 0 & 0.414 \\ 0 & 0 & 0.026 & 0 & 0 & 0.414 & 0 \end{pmatrix} \tag{5}$$

Where

$$\underline{\pi}(k), 0 \le k \le 5$$

is the probability distribution in step *k*. In the above example, according to $\underline{\pi}(4)$, in the 4th step, the probability that VM_2 is compromised will be 2.6% and the probability that VM_7 is compromised will be 41.4%.

5.2. Placement Generation Strategy

Based on the placement strategy generation algorithm shown in Table 1, we have acquired the possibility of being attacked for each VM. Next, we will design a placement strategy to reallocate guest VMs before the attack succeeds. The principle of new strategy is isolating the VMs with high security risks from VMs with low security. In order to reduce the performance overhead, connected VMs with similar security risk will be assigned in the same node. When design the placement algorithm, we assume the node will have enough resources capacity (e.g. CPU, memory and disks etc.) to hold all guest VMs. In each attack step, DTMC and CVSS will predict the attack possibility for each VM. The algorithm will sort the possibility and find the most "dangerous" VM which is most likely to be compromised. The algorithm will assign the most dangerous VM to a dedicated node and allocate other VMs to different node. Therefore, even if the most dangerous VM is compromised, other VM will not be exploited by the attacker. When migrating a VM, the VM is usually shut off first, hence, migration time is one of the most significant factors we should consider in order to improve the system performance. In order to test the overhead on VMs migration, we design an evaluation on the platform specified as Table 1.

Table 1. Algorithm: Placement strategy generation algorithm

```
Require:
 1. Virtual machine set $V = \{V_1, V_2, ..., V_n)$
    Dependent VMs set for each VM set Dependent VMs,
    where dependent $VM_i$ is the set which represents the
 2. Dependent VMs for $VMi$ (i ≤n)
 3. The Physical machine (Node) set $N = \{N_1, N_2, ..., N_k\}$
 4. The compromised possibility for each VM is $Pi$( i ≤ n)
Ensure: Placement Strategy
Sort VMs in ascending order of attack possibility Sort $\{V_1, V_2, ..., V_n)$
dangerous VM = find Most Dangerous ( ) will find the most dangerous VM index by comparing compromised possibility of VMs in set V
dangerous Node = find Random Node ( ) will find a random node to store the dangerous VM.
Mapv (dangerous VM, dangerous Node) will assign dangerous VM to dangerous Node
while! V.empty ( ) do
    node = find Random Node ( ) will return a new node
    new VM = V.pop ( ) find a safe VM
    Map (NewVM, node) assign new VM to safe node
    Map (Dependent new VM, node) assign the connected VMs into same node.
    update V
end while
```

5.3. Result Analysis

According to our experimental results shown in Figure 5, the 91.4% services obtained improved survivability. The maximum survivability enhancement is 74.3% and the average improvement of survivability possibility is 27.2%. In our experiment, we can find there are 20 VMs will be compromised at attack step 1 in random placement plan. However, in our new placement plan, the number of compromised VMs is only 4. Moreover, according to our statistics, the average compromised VM number is 4 in our plan, but in random placement, this average number of compromised VMs is 11.

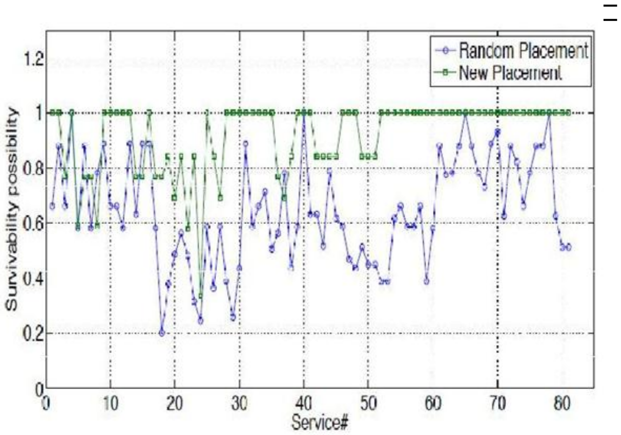


Figure 5. Comparison of survivability

6. CONCLUSION

Cloud computing is quickly becoming more and more important in computing infrastructures. In the migration-based privacy protection approach, we demonstrated that the placement of VMs can make huge difference in terms of security levels. Based on survivability evaluation of VMs and DTMC analysis, we developed an algorithm to generate a safe placement plan that moves the guest VMs before attack succeeds. The experimental results show that our algorithm can significantly improve the survivability of VMs in the cloud and reduce the number of compromised VMs in case of attacks. The overheads of our proposed approach are also practical. In many cases, same vulnerabilities can run on different VMs which will cause adversary to compromise these different VMs simultaneously. Based on our analysis we showed that our proposed algorithm utilizes minimum number of physical servers for hosting the set of VMs, which also reduces the energy consumption of the datacenter and it achieved high resource utilization rate by the way of using minimal number of physical servers. Another considerable enhancement in our algorithm is less percentage of load imbalance value and the percentage of VMs that violate their SLA. The results show that the proposed algorithm can extensively improve the 91.4% of survivability of VMs in the cloud and decreases the compromised VMs numbers in the case of attacks. In our experiment, we can observe 20 VMs will be compromised to 4 at step 1 attack in random and new placement arrangement respectively.

REFERENCES

[1] Thomas Ristenpart et al. *"Hey, You, Get off of My Cloud: Exploring Information Leakage in Third-party Compute Clouds"*, in: Proceedings of the 16th ACM Conference on Computer and Communications Security. CCS '09. Chicago, Illi- nois, USA: ACM, 2009, pp. 199–212. ISBN: 978-1-60558-894-0. doi:10.1145/ 1653662.1653687.url: ttp://doi.acm.org/10.1145/1653662.1653687

[2] Mohammed A. AlZain, Ben Soh, Eric Pardede, "TMR-MCDB: Enhancing Security in a Multi-cloud model through Improvement of Service Dependability," *International journal of cloud computing and services science (IJ-CLOSER)* Vol. 3, No.3, June 2014, pp. 133~144, ISSN: 2089-3337.

[3] Wenjuan Fan, Shanlin Yang, "Multi-Source Information Service (MSIS) Process Management in Cloud Computing Environment," *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, Vol.1, No.1, March 2012, pp. 17~24 ISSN: 2089-3337

[4] Azeem Sarwar, Muhammad Naeem Ahmed Khan, "A Review of Trust Aspects in Cloud Computing Security," *International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Vol.2, No.2, April 2013, pp. 116~122 ISSN: 2089-3337

[5] Z. Mahmood, *"Data Location and Security Issues in Cloud Computing,"* IEEE International Conference on Emerging intelligent Data and Web Technologies, 2011.

[6] A. Behl, *"Emerging Security Challenges in Cloud Computing,"* IEEE international Conference Information and Communication Technologies (WICT), 2011.

[7] D. Chen, H. Zhao, *"Data Security and Privacy Protection Issues in Cloud Computing,"* IEEE International conference on Computer Science and Electronics Engineering, 2012.

[8] K. Popovic, Z. Hocenski, *"Cloud Computing security issues and challenges,"* MIPRO, Proceedings of the 33rd International Convention, 2010.

[9] Siani and Miranda, *"Security Threats in cloud computing,"* 6th international Conference on Internet Technologies and Secure Transactions, 2011.

[10] Hena Shabeeb, N. Jeyanthi, N.Ch.S.N. Iyengar, "A Study on Security Threats in Cloud*," International Journal of*

Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No.3, August 2012, pp. 84~88 ISSN: 2089-3337.

[11] Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, "Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments", 2011 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of [CEIS 2011], Science Direct, pp. 2852 – 2856.

[12] Dimitrios Zissis, Dimitrios Lekkas, "Addressing cloud computing security issues", *Future Generation Computer Systems* 28 (2012),Science Direct 2012, pp. 583–592.

[13] John C. Roberts II, Wasim Al-Hamdani, *"Who Can You Trust in the Cloud? A Review of Security Issues within Cloud Computing",* Information Security Curriculum Development Conference 2011, ACM 2011, pp. 15-19.

[14] John Harauz, Lori M. Kaufman, Bruce Potter, "Data Security in the World of Cloud Computing", IEEE 2009, pp. 61-64.

[15] S. Subashini n, V. Kavitha, "A survey on security issues in service delivery models of cloud computing", *Journal of Network and Computer Applications*, Science Direct , 2011,pp.1-11.

[16] Fahad F. Alruwaili, T. Aaron Gulliver, "SOCaaS: Security Operations Center as a Service for Cloud Computing Environments*," International Journal of Cloud Computing and Services Science (IJ-CLOSER)* Vol.3, No.2, April 2014, pp. 87~96 ISSN: 2089-3337.

[17] Ashish Kumar, "World of Cloud Computing & Security", *International Journal of Cloud Computing and Services Science (IJ-CLOSER)*, Vol.1, No.2, June 2012, pp. 53~58,ISSN: 2089-3337