International Journal of Innovation in Computer Science and Information Technology
Vol.4, NO.1 , P:14 - 25
Received: 20 December 2021
Accepted: 24 January 2022

Overview and Comparing Secure Virtual Machines Algorithms in Cloud Environments

Alireza Karami
Master student, Department of Computer Engineering, Iranian University, Tehran, Iran
alireza.karamii1397@gmail.com

Elham Farahani
PhD in Computer Engineering, Sharif University of Technology
efarahani@ce.sharif.edu

Abstract
Today, in order to reduce energy consumption in the cloud environment, virtualization and dynamic placement of Virtual Machines(VMs) are used, which helps cloud suppliers to reduce energy consumption and maintenance costs of infrastructures and platforms. However, security risks of sharing resources have been identified as one of the main concerns in using cloud computing environments. In particular, an attacker could attack a VM and extend its attack to other VMs that are together in a Physical Machine(PM). The worst-case scenario is when the hypervisor is also compromised, in which case all VMs allocated to the physical node will be at security risk. Therefore, in this study, we have reviewed, categorized and compared the secure algorithms of VM placement, and finally, the shortcomings and challenges in the current algorithms are presented, which can pave the way for the introduction of new secure algorithms.

Keywords: Virtual Machine Placement, Virtual Machines, Security Threats, Algorithms, Cloud Environment, Virtualization

Introduction
The cloud environment in today's world has an important and effective role and provides various services through the network. Cloud service providers Most large data centers are operated by cloud services. Today's data centers are getting bigger and more complex. The applications hosted by these centers are also becoming more complex, and each has a wide range of communication needs. These issues have posed many challenges to resource management in data centers.
Depending on the type of cloud services we use, there is a layer called the virtualization layer, which acts as a powerful technology for the "as a service" pattern and subsequent multiple leasing. This layer enables cloud providers to provide the required service as "pay as you go". Virtualization is the creation of a virtual version of a computational identity. But in cloud computing environments, we especially call virtualization hardware, software environment, network and storage. With hardware virtualization in mind, a host called a VM manager or hypervisor runs on the PM, and on top of this VM manager, there may be several guests or VMs running.
Most VM management methods aim to aggregate the load of VMs on the smallest number of nodes, in order to make more use of computing resources (such as CPU and memory) and to minimize power consumption, while consuming network resources is ignored. This increases network costs and reduces program performance. For this purpose, VMs with high interconnection volume need to be placed close to each other to reduce the communication overhead of the data center network. But the point to be considered in these placement

processes is the issue of security in these placements. One of these security risks in deploying VMs is to attack these deployment processes that try to be in the same place and position with the target client and associate with at least one malicious VM on the same server as the target client, and ddisturb the security of environment.

Therefore, in this paper, we have examined the various security concerns for virtualization as well as the study and comparison of secure VM placement algorithms. In the following, the paper is organized in such a way that in the definitions section, a brief description of key phrases and terms related to the subject of the paper is provided, and in the second section, VM placement algorithms and then security concerns for virtualization are described. In the following, a review of secure algorithms for placing VMs in the cloud environment has been done and the algorithms have been compared and analyzed with each other, and finally the paper ends with a summary and conclusion section.

VM placement algorithms

VM placement is the process of selecting the most suitable PM for a particular VM. Therefore, a VM placement algorithm is used to determine the optimal VM mapping to a PM. Whether it is initial VM placement or VM migration for location optimization. The VM placement method can have one of two purposes: Based on the intended purpose, VM placement algorithms can be generally classified into two types:

1- Energy-based approach: with the aim of achieving a map for VM mapping to the PM, which leads to the creation of a system with energy savings and also with maximum use of resources

2- Higher quality-based approach in service: with the aim of achieving a map for VM mapping to the PM with the assurance of achieving the maximum quality of services required

Table1 lists the types of approaches to VM placement algorithms

Table 1: Classification of VM placement algorithms types

Different Types	Description
Accurate - Exploring – Learning machine	Types of approaches
Static - Dynamic	Time of decision making
Use of Resources - Network Traffic - Reliability - Immigration Overhead	Decision parameters
Number of Ready-Made Hosts - Energy Consumption - Service Level Agreements - Fine Error-Reliability - Load Balance	Evaluation goals
Simulation Tools - Real Implementation	Evaluation environment

Security concerns for virtualization

Recently, security risks in cloud computing are similar to the old security risks. But technologies used to empower cloud services may provide other security risks that are for cloud operational model. According to a recent report published by the Alliance of Cloud Security, joint technology vulnerabilities along with cloud security threats, such as account theft, insecure interfaces, and data rape as common and main security risks in a cloud computing environment. Are considered.

In cloud computing environments, the virtualization layer uses common technologies so that cloud suppliers can be actively IaaS, PaaS and SaaS. Virtualization is a general issue that includes many concepts and technologies. Virtualization is currently used at hardware and software levels. The term virtualization is often used instead of hardware virtualization and plays a more prominent role in providing IAAS services. Virtualization to the cloud supplier, the power supply of self-service computing resources and required. But exploiting this

technology as the main support of cloud data centers also increases security risks. This is because this technology uses software resources and common hardware that can endanger the user's assets and privacy if it is not properly separated. So far, various security attacks about virtualization technology are introduced. In Table 2, these attacks are summarized and explained

From the list of attacks shown in Table 2., an attacker can use security vulnerabilities in the virtualization layer to exploit other or hypervisor VMs. An attacker can directly attack a VM and access to VM, or even rent a VM in the cloud supplier infrastructure and attack it VM. After that, the attacker has several possible. He can attack other VMs by exploiting a number of vulnerabilities, attacking other VMs, or use common memory to carry out adjacent channel attacks. If the attacker can jeopardize the self-help, then all VMs are available.

Table 2: Types of virtualization layer attacks

Attack Type	Description
Communication between VMs[26]	If the cloud provider does not consider a security mechanism for separating VMs, the attacker can transmit data between VMs that are in a host.
VM monitoring through the host[28]	The host can change resources as well as guest VMs. Therefore, the host access to an intruder allows full access to VMs
VM attack to VM [29]	If the security mechanism is compromised, the attacker can achieve the authority of guidance and endanger other VMs
Attack on lateral channels[30]	The attacker can put a malicious VM on the host and attack itself by accessing their virtual VM
Escape from VM [31]	The attacker escaped from the sandbox created by hypervisor
Attack in hypervisor[32]	The attacker tries to control VMs by exploiting the vulnerability of hypervisor
Virtual bottle[26]	Using scanning tools, the attacker can identify vulnerable VMs for botnets deployment
Injection attacks of virtual code[26]	If the cloud provider does not provide a good security mechanism, the attacker can inject malicious code to the virtual environment
Breakout attack[33]	The attacker can jeopardize VM and open a communication channel to another VM that deployed in the same host
Memory memory leakage[34]	Sometimes, when the host is at allocating or liberalization of common memory, a system failure occurs, which can cause virtual memory leakage

Security Assessment

In this section, the security assessment is particularly referred to assessing risks in relation to VMs and PMs in the cloud computing environment. US National Vulnerability Database (NVD) is used to identify and determine vulnerabilities in each VM [35]. In NVD, all vulnerabilities are scored according to the Common Vulnerability Scoring System (CVSS) [36].

Should understand the concept of CVSS. CVSS provides an open framework for displaying the main features of various software vulnerabilities and provide a numeric score that shows its intensity. Then the numerical score can be interpreted as a qualitative display (such as low, moderate, high and critical) to help companies evaluate their proper vulnerability management processes. CVSS is used by various global companies to evaluate the vulnerabilities in their

systems, and respond to vulnerabilities encountered in daily operations. CVSS is currently maintained by the Association of Security Team and Response to FIRST [37].

The three metric groups are used to produce CVSs. The first is the base score that is a compulsory option and shows the intensity of assumed vulnerability. The second metric group is a metric when an optional metric and measures the effect of development, such as the release of time or code for exploitation. The third group is environmental metrics that are an optional metric, which allows the evaluation of the effect with the potential loss based on the expectations of the victim system [36]. Since environmental scores and time are completely optional metrics for CVSS scores and used to customize the CVSS score for a specific organization and deployment environment, we only consider the base score in this study.

The base metric group consists of two metric sets: (1) Metrics of operation and (2) effects metrics. The exploitation metrics show the skill and coherence of the attacker to exploit the assumed vulnerability. On the other hand, the metrics of the effect show the direct effect of the vulnerability on the asset. Common Calls and Vulnerability System (CVE) [38] provides a dictionary that determines a unique identifier for all security vulnerabilities known as public. CVE is maintained by Miter (MITRE) [38]. When a vulnerability is detected, a separate CVE identifier is given to it and a brief description of the vulnerability is also given to it. In other words, NVD is a reservoir that stores CVSS scores for all CVE vulnerabilities. So far, NVD keeps information about more than 126,000 CVE vulnerabilities. These vulnerabilities now include the latest attacks on cloud computing environments, especially those affiliated with the virtualization layer. Since the NVD website provides XML files dependent on CVE records, researchers can use this data to identify VM vulnerabilities as well as evaluate and examine their proposed methods.

An overview of secure algorithms of VM placement in the cloud environment

Regarding the increasing number of strategies to carry out side attacks through VM, security environments have become a concern. The attacks allow the enemy to steal private information from a target user that VM is in a common position with enemy information. Therefore, in this section focuses on the related work of the past, which is based on the secure VM algorithms, and the summary of each one is expressed.

Recent work [4.3] focuses on increasing electricity productivity and thus reducing the cost of data centers. However, the problem of increasing resource productivity while maintaining security security is still a major issue. A simple way to reduce side attacks and other accumulation-based attacks, assign a proprietary PM to any cloud user. Although this cancels the chance of shared location-based attacks, it also affects the use of cloud data center resources. Assigning a dedicated PM for each cloud user leads to a large number of unemployed cores in live PM, which in turn increases the cost of data center energy. Therefore, defense strategies need to be designed to be able to deal with location-based attacks without significant increase in the cost of office. In this section, some defenses against location-based attacks that are proposed over the years and review the benefits and disadvantages. Most ideas can be classified in general to two main categories:

(1) Reduce information leakage through the available side duct
(2) Reduce the probability of attacking attackers with cloud users.

We discuss the proposed solutions for each of the two expressed categories in the following sections

(1) Reduce information leakage through the available side duct

The main purpose of the actions taken in this category is to modify architecture (hardware, operating system, hypervisor, etc.), so that the side channels deleted or reduce the amount of information leakage through lateral channels.

Regarding the prevention projects of the adjacent channel attack, Lee et al. Takes IaaS. This method allows you to view accumulated scheduling information for these VMs.

In [2], the authors proposed to fight time-based channels by modifying the RDTSC instruction that provides accurate timing information in Xen machines.

Wang et al. [6] The new architecture of cache suggests that the security algorithm uses the SECRAND to deal with side channel attacks.

Liu et al. [7] Designed a random cache storage architecture that, in addition to defense against dispute-based attacks (for example, Prime-Probe, Evict-Time), also provides security against reuse-based attacks. Slow (eg, Flush-Reload, Cache-Collision) suggests the use of a customizable cache architecture that can protect the dynamic division of cache to protected areas against lateral attacks.

Wang et al. [9] Safe virtual network plan to combat information leakage through secret channels in the virtual network environment.

Lee et al. [10] suggested a hypervisor-based defense system that aims to obscure leakage time information in the IAAs clouds using 3 replications of each VM and only allowed to view the overall timing information of these VMs.

Varadajan et al. [11] was proposed to defend counter-channel-based channel attacks by reducing the frequency of the VM prediction that is controlled by the Hypervisor planner.

Zhang and his colleagues offered a system called Duppel, which allows a VM to defend itself against the adjacent channel attack in the clouds. In this way, VM will inject noise to schedules that an attacker may see from the cache. Dopel does not need any changes to hyperviser or cloud suppliers.

Vatikunda and colleagues [5] suggested a method for removing adjacent timing channels by modifying the RDTSC recipe data that produces fine-line data in VMs -Xen. The main loss of all of these methods is that they do not consider other types of attacks such as VM escape.

Patock et al. [13] Designed a system that prevents the keys of encryption keys in common cloud environments by dividing the key in several VMs

(2) Reducing the likelihood of invaders with cloud users

The primary purpose of the works in this category is to design ways to prevent or reduce the likelihood of a malicious user with a benign user. Creating a common location is the main prerequisite for side attacks (and other location-based locations). Therefore, a VM strategy prevents (or reduces malicious consolidation) directly reduces the chance of a successful attack. There are two different ways that can be reduced by them as a common location:

(1) With the design of secure VM algorithms

(2) With the design of safe immigration strategies VM

In relation to the VM, Yachi and colleagues [37] plan, they have proposed a method for considering security risks for the decision-making process of VM. In this method, in the first step, the dose of all VMs and PMs is calculated, and based on calculated scores, scheduler decides which VM should be in a particular PM. In this particular study, for ease of decision-making process, calculated scores have been translated into three different groups: (1) lower, (2) average, and (3) high degrees. The main advantage of this study is that the proposed algorithm considers security assessment for VMs and PMs. Nevertheless, this study only considers the security agent as its ultimate goal, and other factors do not consider other factors such as network traffic, energy consumption and so on. Also, one of the main assumptions of this work is that the set of unlimited resources is available.

In another VM plan, Agaral and Dong [39], algorithm suggested that the design of the first users already in one place (PCUF) is called. In

this study, with the assumption of a new VM, Scheduler checks if the user is a new user and also did he get a VM in the past or not. If the user is a new user, the algorithm randomly chooses a PM to reduce user hostile activities. But if the user is an old user, then based on the availability of PMs, the algorithm tries to assign a PM that has previously been assigned to VM users. This, in addition to the advantages listed, has its own limitations. First, it only considers newly added VMs and does not consider old VM for immigration based on necessity or demand. Secondly, the location of all VMs for a particular user may increase attack risks for that particular user. This user may be a company and some of its VMs may include vulnerabilities. So, the location of those VMs can potentially be a high-risk decision for the company.

Also, Han and his colleagues [40] offered a multi-purpose method called the VM platforming algorithm based on the optimization of the Smoop. This algorithm considers three targets for optimization: (1) security risk, (2) source waste, and (3) network traffic. One of the advantages of this method compared to the rest is that cloud suppliers can expand their goals and define new constraints, such as the cost of immigration or energy consumption, based on their preferences. Of course, there are still a set of shortcomings. For example, hesitation and uncertainty are not considered in calculating the above goals. Also, the priority of these goals is another important point not reflected.

In the valuable VM placement plan, his harassment and colleagues suggested a method that accidentally puts a VM in a physical car. All PMs in the data center must have a label and the label is assumed or "open, closed or blank". The open label means the PM has previously received a number of VMs and can host more VMs. The closed label means the PM is full and cannot host another VM. Finally, the empty label shows a PM that has not received any VM yet. To select the appropriate physical server for a new VM, scheduler randomly chooses an open PM. If the assumed PM fails to accept additional VMs, then its label changes to the closed label. Also, one of the PMs with the empty label will again be labeled and takes the open label. The main advantage of this study is to consider different PMs to allocate a new VM. In this way, an enemy user cannot be sure about their victims. Although the random distribution of VMs in the first place looks good, for some PMs, the level of accumulated vulnerability may be high and this can increase the security risk of those PMs

A group-based placement plan for VM was first studied by Liang et al. [41]. In order for this method to produce the design appropriately, a metric was created as the probability of simultaneous residence. While this research on the Cloudsim platform, no risk analysis or attack has been done.

Karun and his colleagues [42] argue that customers should be able to determine their security conditions. However, the lack of accurate security metrics leads to inability to determine the level of security of the establishment of a customer in a cloud computing environment. To eliminate this, the authors, integrated and comprehensive security metrics provide computational nodes as well as communication links. Later, the user can choose between the above metrics and decides the placement algorithm about which VM should be assigned to which PM. In addition to the advantages of this solution, it is clear that security metrics ignore security risks due to simultaneous allocation of VMs.

A recent study was introduced by Javar and his colleagues [43] a method of mapping limitation. The proposed model suggests a placement limitation based on cloud supplier and user profile. Placing limitations are divided into three types: (1) National constraints applied to all PMs and VM, (2) infrastructure constraints set by cloud supplier to provide security and service quality, (3) Optional limits that are determined by users to strengthen the security of the applications. The most important limitation of this study is a lack of attention to resource allocation.

L-Hajj et al. [44] suggested a method for creating various security groups for VM based on the similarity of their accessibility conditions as well as the risk of a specific VM for the assumed group. The authors for its formulation show the allocation of safe resources as a limitation problem (CSP) [45]. To solve this, the modulus (modulus) theories are applied (SMT) [46]. In addition to the advantages of the proposed model, the authors formulate this as a CSP and not as an optimization problem. According to it, the proposed solution can be used in areas where the removal of input constraints is prioritized and may not be efficient in situations where optimal decisions are needed. In other interesting research, Yu et al. [47] suggested a method for providing immigration and placement plan based on China's wall policy. Before initiating the production of the plan, the aggressive benefit conflicts were measured for each user. Following this, the rules of isolation (isolation) were applied, and finally, the VM placement algorithm moved VM to the appropriate PM. While this method is more concerned about the separation of VMs according to the VM users, the actual cost of exploitation of the source has not been considered.

Zhang et al. [22] "Cloudradar" suggested as a system for detecting side attacks through the communication of abnormal striker cache activities with the activity of the encryption program of a user. They used signature-based diagnostic schemes to identify the user's implementation of some encryption programs and anomalies based diagnostic designs to identify unusual cache control of a potential attacker. They also used hardware function counters in modern CPUs to collect and monitor the cache of cloud users.

Similarly, Chiapte et al. [21] Methods for using hardware counters with techniques such as correlation-based approach, anomalous detection and monitoring learning to detect Flush + Reload-based side attacks in real time Described.

The universe and his colleagues used several types of categories, including but not limited to, Naive Bayes and Support Vector Machine. These possible categories about input features related to the detection of side channel attacks such as Branch errors, LLC Misses, LLC references, main cycles without restrictions, number of instructions, etc. and later for classifying an activity Unknown as benign or destructive.

Ahmed et al. [24] proposed a way to create security profiles for VMs by combining various parameters such as internal vulnerability score, intrusion behavior score and trust-based score. The weighted average of these scores was used to construct the Security Specification Score (SPS). These mechanisms can be used by the cloud provider to actively monitor tenant activity and determine whether a particular tenant is aggressive or does not use a classification system.

Han et al. [14] A model based on the theory proposed to compare the security of various policies of placement VM against location attacks.

In [15], they also suggested a new allocation policy with the previous name of the servers (PSSF), aimed at reducing the probability of location by minimizing the expansion of VMs requested by the user.

Bryma et al. [16] has proposed a location algorithm that aims to reduce the location of the location by compromising VM launch times instead of optimizing resources. Their strategy uses the preset mixing queue in which VM requests are buffered. The actual replacement only begins after the queue filling by selecting a random VM from the queue and assigns it to a physical server according to the optimization strategy.

Kiu et al. [17] suggested a resistance strategy against VM based on custom defined threshold parameters. Their strategy considers these threshold parameters and focuses on the policy "first expand, focus later, and the more VMs create more".

Folki et al. [18] suggested a secure deployment policy by placing a trust relationship between cloud users. This freedom is given to any user to select the collection of its enemies, and this is considered when it decides on the location.

Zhang et al. [19] suggested a virtual machine-friendly immigration strategy based on animated defense philosophy to combat station-based attacks.

Moon et al. [20] The cloud provider suggested the VM migration strategy to limit the joint presence and limiting the amount of information leakage due to side channel attacks.

Analysis of past approaches

For better comparison, we summarize the features browsed in this section in Table 3. The parameters that are considered for comparison are as follows:

1. The participation of cloud suppliers is required or user participation
2. Methods used to identify vulnerabilities
3. Considering other placement indicators
4. VM placement based on a random design

Table 4 provides a summary of the benefits, disadvantages and progress related to past tasks at high levels.

Table 3. Comparison of related work based on defined indicators

Random design	Considering other indicators	Vulnerability identification method	User participation	Method	Category
×	×	CVSS, NVD, CVE	✓	Yachi and colleagues	VM. Placing Method
✓	✓	-	×	Agaral and colleagues	
✓	✓	CVSS, NVD, CVE	✓	Han and colleagues	
×	×	-	✓	Azar et al	
✓	×	-	✓	Karun and colleagues	
×	✓	CVSS, NVD, CVE	×	L-Hajj and colleagues	
×	×	-	✓	Jewel and colleagues	
×	✓	-	×	Yo and colleagues	
×	×	-	×	Liang et al	
×	×	-	×	Lee et al	Wash preventing data leakage through lateral channels
✓	×	-	×	Zhang et al	
×	×	-	×	Vatikonda et al	

Table 4: Analysis of previous related work

Category	Possible Improvements	Limitations	Advantages
Special defense of architecture [13–5]	The design of generalized techniques that can handle future side channels while the need for minimum hardware / software changes.	Requires basic changes in existing cloud infrastructure and does not guarantee security against current unknown side canals.	Effective in reducing information leakage through lateral channels available by modifying operating system, cache, hypervisor, network and so on.
VM location-based defense [20–14] ,[1]	Use of VM cache statistics to ensure further separation of attackers while ensuring high resource use.	Affects the use of data center resources. Immigration-based defense incurs an additional network cost for the cloud provider.	Effective in reducing the likelihood of malicious and resistant to arbitrary side canals

Summary and Conclusion

This paper reviews, categorized and compared safe algorithms of VMs placement. Most described algorithms in this section suffer from two basic constraints that prevent them from accepting the current cloud architecture: 1) They need major changes in existing cloud infrastructure such as hypervisor and guest operating system and physical hardware have. 2) They do not guarantee security against current unknown side channels**.**

Compared to hardware-based defense systems described in this paper, described strategies may be more appropriate and more practical than in two main environments: 1. Unlike defensive systems Hardware-based, they do not need to have basic changes in the cloud infrastructure. 2. Probably against arbitrary attacks and currently unknown side canals are more resistant.

However, these solutions have some common shortcomings: (a) Resolution algorithms significantly affect the use of cloud data center sources. (B) Immigration-based defenses suffer additional network costs for cloud provider. (C) Most of the proposed strategies have not been evaluated on the real-world working dataset.

As future work, it is proposed to provide a secure virtual machine placement algorithm to reduce the risk of co-location for vulnerable virtual machines to cover all the shortcomings mentioned above.

References

[1] Y. Azar, S. Kamara, I. Menache, M. Raykova, B. Shepard,(2014), Co-locationresistant clouds, in: Proceedings of the 6th Edition of the ACM Workshop on Cloud Computing Security, ACM, 2014, 9–20.

[2] E. Cortez, A. Bonde, A. Muzio, M. Russinovich, M. Fontoura, R. Bianchini,(2014),Resource central: Understanding and predicting workloads for improved resource management in large cloud platforms, in: Proceedings of the 26th Symposium on Operating Systems Principles, ACM, 153–167.

[3] Z. Guo, Z. Duan, Y. Xu, H.J. Chao,(2014), JET: Electricity cost-aware dynamicworkload management in geographically distributed datacenters, Comput.Commun. 50,162–174.

[4] Z. Guo, S. Hui, Y. Xu, H.J. Chao, (2016), Dynamic flow scheduling for power-efficientdata center networks, in: Quality of Service (IWQoS), 2016 IEEE/ACM 24thInternational Symposium on, IEEE, 1–10.

[5] B.C. Vattikonda, S. Das, H. Shacham,(2011) Eliminating fine grained timers in xen, in: Proceedings of the 3rd ACM Workshop on Cloud Computing SecurityWorkshop, ACM, 41–46.

[6] Z. Wang, R.B. Lee, (2008), A novel cache architecture with enhanced performanceand security, in: Proceedings of the 41st Annual IEEE/ACM InternationalSymposium on Microarchitecture, IEEE Computer Society, 83–93.

[7] F. Liu, R.B. Lee, (2014), Random fill cache architecture, in: Microarchitecture(MICRO), 2014 47th Annual IEEE/ACM International Symposium on, IEEE, 203–215.

[8] D. Page,(2008) Partitioned Cache architecture as a side-channel defencemechanism, IACR cryptology eprint archive

[9] Z. Wang, J. Wu, Z. Guo, G. Cheng, H. Hu, (2016), Secure virtual network embeddingto mitigate the risk of covert channel attacks, in: Computer CommunicationsWorkshops (INFOCOM WKSHPS), 2016 IEEE Conference on, IEEE, 144–145.

[10] P. Li, D. Gao, M.K. Reiter,(2014), Stopwatch: a cloud architecture for timingchannel mitigation, ACM Trans. Inf. Syst. Secur. (TISSEC) 17 (2)

[11] V. Varadarajan, T. Ristenpart, M.M. Swift,(2014), Scheduler-based Defenses agains Cross-VM Side-channels, in: USENIX Security Symposium, pp.687–702.

[12] Y. Zhang, M.K. Reiter, (2013), Düppel: retrofitting commodity operating systemsto mitigate cache side channels in the cloud, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, ACM, 827–838.

[13] E. Pattuk, M. Kantarcioglu, Z. Lin, H. Ulusoy, (2014), Preventing cryptographic keyleakage in cloud virtual machines, in: USENIX Security Symposium, 703–718.

[14] Y. Han, T. Alpcan, J. Chan, C. Leckie,(2013), Security games for virtual machine allocation in cloud computing, in: International Conference on Decision and Game Theory for Security, Springer, 99–118.

[15] Y. Han, J. Chan, T. Alpcan, C. Leckie, (2017), Using virtual machine allocation policies to defend against co-resident attacks in cloud computing, IEEE Trans. Dependable Secure Comput., Vol.14, No.1, 95–108.

[16] M. Berrima, A.K. Nasr, N. Ben Rajeb, (2016), Co-location resistant strategy with full resources optimization, in: Proceedings of the 2016 ACM on Cloud Computing Security Workshop, ACM, 3–10.

[17] Y. Qiu, Q. Shen, Y. Luo, C. Li, Z. Wu,(2017), A secure virtual machine deployment strategy to reduce co-residency in cloud, in: Trustcom/BigDataSE/ICESS, 2017 IEEE, IEEE, 347–354.

[18] Z. Afoulki, A. Bousquet, J. Rouzaud-Cornabas, (2011), A security-aware scheduler for virtual machines on iaas clouds, http://www.univ-orleans.fr/lifo/ prodsci/rapports/RR/RR2011/RR-2011-08.pdf.

[19] Y. Zhang, M. Li, K. Bai, M. Yu, W. Zang, (2012), Incentive compatible moving target defense against vm-colocation attacks in clouds, in: IFIP International Information Security Conference, Springer, 388–399.

[20] S.-J. Moon, V. Sekar, M.K. Reiter, (2015), Nomad: Mitigating arbitrary cloud side channels via provider-assisted migration, in: Proceedings of the 22nd Acm Sigsac Conference on Computer and Communications Security, ACM, 1595–1606.

[21] M. Chiappetta, E. Savas, C. Yilmaz, (2016), Real time detection of cache-based sidechannel attacks using hardware performance counters, Appl. Soft Comput.,49 ,1162–1174.

[22] T. Zhang, Y. Zhang, R.B. Lee, (2016) Cloudradar: A real-time side-channel attack detection system in clouds, in: International Symposium on Research in Attacks, Intrusions, and Defenses, Springer, 118–140.

[23] M. Alam, S. Bhattacharya, D. Mukhopadhyay, S. Bhattacharya, (2017), Performance counters to rescue: A machine learning based safeguard against micro-architectural side-channel-attacks.

[24] F. Ahamed, S. Shahrestani, B. Javadi, S. Garg,(2015), Developing security profile for virtual machines to ensure secured consolidation: conceptual model, in: Proceedings of the 13th Australasian Symposium on Parallel and Distributed Computing (AusPDC 2015), Held in Parramatta, Sydney, Australia, 27-30.

[25] T.Yarygina, A.Bagge, (2018), Overcoming security challenges in microservice architectures. In: IEEE symposium on service-oriented system engineering (SOSE), Bamberg, Germany, 37–42

[26] C.Modi, K.Acha, (2016), Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review. J Super comput, Vol.73, No.3 ,1192–1234

[27] Top Threats to Cloud Computing: Deep Dive (2018) https ://cloud secur ityal lianc e.org/artif acts/top- threa ts-to-cloud -compu ting-deep-dive/. Accessed Date 14 Oct 2020

[28] C.Lita, D.Cosovan, D.Gavrilut, (2017), Anti-emulation trends in modern packers: a survey on the evolution of anti-emulation techniques in UPA packers. J Comput Virol Hack Tech 14:107–126

[29] D.Kadam, R.Patil , C.Modi, (2018), An enhanced approach for intrusion detection in virtual net-work of cloud computing. In: Proceedings of the 10th International Conference on Advanced Computing (ICoAC), Chennai, India, 80–87

[30] S.Bhunia, M.Tehranipoor, (2019), Security and trust assessment, and design for security Hardware, 13:347–372

[31] J.Wu, Z.Lei Z, S.Chen, W.Shen, (2017), An access control model for preventing virtual machine escape attack. Future Internet, Vol.9, No.2, 20–37

[32] S.Rama Krishn, B.Padmaja Rani, (2016), Virtualization security issues and mitigations in cloud computing. In: Proceedings of the 1st International Conference on Computational Intelligence and Informatics, HeydarAbad, India, 117–128
[33] M.Dildar, N.Khan, J.Abdullah, A.Khan, (2017), Effective way to defend the hypervisor attacks in cloud computing. In: Proceedings of the 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, 154–159
[34] S.Li, J.Koh, J.Nieh, (2019) Protecting cloud virtual machines from hypervisor and host operating system exploits. In: Proceedings of the 28th USENIX security symposium, California, USA, 1357–1374
[35] NVD—Home. https ://nvd.nist.gov. Access date 24 Nov 2019
[36] Common Vulnerability Scoring System SIG. https ://www.first .org/cvss/. Accessed date: 24 Nov 2019
[37] X.Yuchi, S.Shetty, (2015), Enabling security-aware virtual machine placement in IaaS clouds. In: IEEE military Communications Conference, Tampa, FL, 1554–1559
[38] CVE—Common Vulnerabilities and Exposures (CVE). https ://cve.mitre .org/. Accessed date: 24 Nov 2019
[39] A.Agarwa, T.Duong, (2019), Secure virtual machine placement in cloud data centers.Future Gener Comput Syst 100:210–222
[40] J.Han J, W.Zang, S.Chen , M.Yu, (2017), Reducing security risks of clouds through virtual machine placement. In: Proceedings of the data and applications security and privacy XXXI, Philadelphia, PA, USA, 275–292
[41] X.Liang, X.Gui, A.Jian, D.Ren, (2017), Mitigating cloud co-resident attacks via grouping-based virtual machine placement strategy. In: Proceedings of the 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), San Diego, CA, 1–8
[42] E.Caron, J.Cornabas, (2014), Improving users' isolation in IaaS: virtual machine placement with security constraints. In: Proceedings of the 2014 IEEE 7th International Conference on Cloud Computing, AK, USA, 64–71.
[43] R.Jhawa, V.Piuri, P.Samarati, (2012), Supporting security requirements for resource management in cloud computing. In: Proceedings of the 2012 IEEE 15th International Conference on Computaional Science and Engineering, Nicosia, Cyprus, 170–177
[44] S.Al-Haj, E.Al-Shaer, H.Ramasamy, (2013), Security-aware resource allocation inclouds, In: Proceedings of the 2013 IEEE International Conference on Services Computing, Santa Clara, CA, USA, 400–407
[45] A.Bulato, V.Guruswami, A.Krokhin, D.Marx , (2016) The constraint satisfaction problem: complexity and approximability. Dagstuhl Rep, Vol.5, No.7, 22–41
[46] C.Barrett, C.Tinelli, (2018) Satisfiability modulo theories. In: Handbook of model checking. Springer, Cham, 305–343. https ://doi.org/10.1007/978-3-319-10575 -8_11
[47] S.Yu, X.Gui, J.Lin, F.Tia, J.Zhao, M.Dai, (2014), A security-awareness virtual machine management scheme based on Chinese wall policy in cloud computing. Sci World J 2014:1–1242.
[48] P.Li, D.Gao, M.Reiter, (2013), Mitigating access-driven timing channels in clouds using StopWatch. In: Proceedings of the 2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Budapest, Hungary, pp 1–12.