ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

A Study on Virtualization Techniques in Cloud Computing

Dr.Chintagunta Mukundha, O.Sahithi Reddy, L.Tejasri

Associate Professor, Dept. of IT, Sreenidhi Institute of Science & Technology, Hyderabad, India

UG Student, Dept. of IT, Sreenidhi Institute of Science & Technology, Hyderabad, India

UG Student, Dept. of IT, Sreenidhi Institute of Science & Technology, Hyderabad, India

ABSTRACT: Cloud computing technology is one of the next generation technologies booming up business and IT field. It can be used anywhere and anytime. It provides on demand IT services and helps to overcome the problems of data loss, accessing data whatever or whenever needed and data security. This technology mainly focuses on cost reduction, hardware reduction, pay-per-use business model, scalability and flexibility in computer services. As the number of existing cloud vendors rises, resource count and types are ever increasing leading to a need of cloud management solutions. While providing several services, cloud management's primary role is resource provisioning. In order to meet application needs in terms of resources. The central part of cloud computing is virtualization which enables resources through on-demand allocation dynamically. Virtualization is a technique that creates a virtual image of storage, software and server resources so that they can be used on multiple machines at the same time. The resources have different forms such as network, server, storage, application and client. It does so by assigning a logical name to a physical resource and providing a pointer to that physical resource on demand. . In this paper the virtualization approach in the cloud computing environment are well presented with the concept of the cloud service models. It also gives a detailed review on how virtualization works, and its advantages, future scope and challenges.

KEYWORDS: security, virtualization, resource provisioning, storage.

I. INTRODUCTION

Traditional infrastructure provisioning model is inefficient and does not meet the requirements of the internet era. But Cloud computing leads to an innovative approach in the way in which IT infrastructures, applications, and services are designed, developed, and delivered. National Institute of Standards and Technology (NIST) has given a definition for Cloud computing which says "Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort". Five essential characteristics of cloud computing listed by NIST are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

Mobile cloud computing is the computing which refers to anytime, anywhere accessibility to applications and data through internet using mobile devices. Traditional computing resources are stored in an individual device and accessed by an authenticated user. In Cloud computing, resource are stored in centralized manner and accessed on demand basis. In recent days, mobile devices and subsequent mobile computing became an imperative component in cloud computing. In cloud computing one uses the service over internet rather than keeping data in hard drive and regularly updating the applications. Thus it is observed that there is a significant change in workload. The computers make up the cloud handles the workload instead. The hardware and software demands are decreased. An interface software like web browser is the only thing required by the user's computers and rest care is taken by the cloud's network. Thus it is also known as "internet based computing".

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

These services are used by software industries, government sectors, and health care sectors and in many more fields. This vision opens new opportunities that significantly change the relationship that enterprises and end-users have with software and technology. Apple, Google, Microsoft, etc. are the biggest cloud service providers who provide very large storage to its users by making the work easier.

The main aim of virtualization is to manage the workload by transforming traditional computing to make it more scalable, efficient and economical. Virtualization technology diverts the human's perspective for utilizing IT resources from physical to logical. Virtualization is a technique which allows to create abstract layer of system resources and hides the complexity of hardware and software working environment. It creates a virtual image of something such as server, operating system, storage devices or network resources so that they can be used on multiple machines at the same time so to reduce the cost of IT resources. The resources can be allocated or altered dynamically. It is rapidly transforming the fundamental way of computing. The virtualization provides hardware independence, isolation of guest operating system and encapsulation of entire virtual machine. Virtualization can be applied to a wide range such as operating system virtualization, hardware-level virtualization and server virtualization. It is mainly implemented with the help of a hypervisor. Even though cloud computing can exist without virtualization but it may be inefficient and difficult for the users. The IT world is looking forward for the services provided by cloud computing thus boosting up the development of cloud computing.

II. RELATED WORK

Pearson (2009) is talking in depth about privacy issues in cloud computing, nominal cloud security issues are discussed in the literature review of Gu and Cheung (2009). Siebenlist (2009) has discussed some interesting features in cloud security issues, Cachin at al(2009) made a complete survey on security in the context of storage services in the cloud . An exhaustive assessment has been made by Enisa(2009) in the area of cloud security assessment. Armbrust et al. (2009) made a worthy survey on cloud computing, Mukundha[2016] has discussed some of the security problem in the cloud security. All the above papers have been the starting points of our work and we refer to them in terms of problems and terms definition. A fundamental reference for our research is the work on co-location (Ristenpart, 2009) by Ristenpart. It describes that is it a possible way to instantiate an increasing number of guest Virtual Machines until one is placed co-resident with the target Virtual Machine. Once co residency is successfully achived, then attacks can extract information from a target Virtual Machine on the same machine. An attacker might also actively trigger new victim instances exploiting cloud auto-scaling systems. Ristenpart shows that it practical to hire additional VMs whose launch can produce a high chance of co-residence with the target Virtual Machine. He also shows that determining co-residence is quite simple.

Majority of the current existing intrusion detection and integrity monitoring solution can be applied successfully on the cloud computing. File system Integrity Tools and Intrusion Detection Systems such as Tripwire (Kim and Spafford,1994) and(AIDE) (AIDE team, 2005) can also be deployed in virtual machines, but are exposed to attacks possibly coming from a malicious guest machine user. Furthermore, when an attacker identifies that the targeted system is existed in a virtual environment ,it may attempt to breakout of the virtual environment through the vulnerabilities that are existing in the virtualization(very rare at the time of writing Secunia, 2009) in the Virtual Machine Monitor(VMM). Most present approaches leverage VMM isolation properties to secure VMs by leveraging various levels of virtual introspection. Virtual introspection (Jiang etal.,2007) is a process that allows to observe the state of aVM from the VMM. SecVisor (Seshadri etal., 2007) Lares (Payne etal.,2008) and KVM-L4 (Peter etal.,2009), to name a few, leverage virtualization to observe and monitor guest kernel code integrity from a privileged VM or from theVMM. Nickle (Riley etal. 2008) aims at detecting kernel root kits by monitoring the integrity of kernel code. However, Nickle does not protect against kernel data attacks (Rhee etal.,2009), where asour solution does.Most proposals have limitations that prevent them from being used in distributed computing scenarios(e.g.. SecVisor only supports one guest per each host)or just do not consider the special requirements or peculiarities of distributed systems; for instance, KVM-L4 shares the same underlying technology as Lombardi and DiPietro(2009) but the additional context switching overhead in the64-bit scenario, representing the vast majority of cloud hosts, remains to be verified.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

Also worth citingare IBM on (Ranadive etal., 2009), a monitoring utility using introspection for asynchronous monitoring of virtualized network devices, and Low Grid (Salza etal.,2006), an example of autonomic reaction system. In an effort to make nodes resilient against long-lasting attacks, Self-Cleansing Intrusion Tolerance (SCIT) (Huang etal., 2006) treats all servers as potentially compromised(since undetected attacks are extremely dangerous overtime). SCIT restores servers from secure images on a regular basis. The drawback of such a system is that it does not support long-lasting sessions required by most cloud applications .Similarly, VM-FIT (Distler etal.,2008) creates redundant server copies which can periodically be refreshed to increase the resilience of the server. Finally, Sousa etal.(2007) approach combines proactive recovery with services that allow correct replica store act and be recovered when there is a sufficient probability that they have been compromised. Along with the many advantages brought by virtualization, there are additional technological challenges that virtualization presents, which include an increase in the complexity of digital forensics (Pollitt etal., 2008) investigations as well as questions regarding the forensics boundaries of a system.

III. VIRTUALIZATION IN CLOUD

Most of the businesses often use a combination of a number of application servers, web servers, image servers, file servers, video and audio servers, and the database servers. Generally ,the amount of time the server machine is kept up and running relative to the actual time spent by it servicing the requests, is much higher .This clearly shows that a significant amount of energy is wasted per server in the process of keeping the servers up and ever-ready to service requests upon their arrival.. For ensuring that a good fraction of time is spent by the server in servicing requests, virtualization must be ensured. Virtualization technology makes cloud computing environment easily to manage the resources. Virtualization technique ensures the availability of hardware to each and every user, the details of the virtual, simulated environment are kept transparent from the application. It facilitates Isolation among users i.e, Every single user is isolated from other users so that they doesn't get information about the other user's data and usage and they can't access other's data. The other benefits of virtualization are stated below:

a. **Resource sharing:**
A much larger resource can be fragmented into multiple virtual resources so that they can be used by multiple users using virtualization technique.

b. **Dynamical resources:**
Reallocation of resources such as storage and computational resources are very difficult but if they are virtualized then they can be easily re-allocated.

c. **Aggregation of resources:**
The smaller resources available can be increased at a larger extent with the help of virtualization.

d. **Reduces the cost:**
As virtualization reduces the number of physical servers as a result of which one needs to maintain few servers ,this becomes much cheaper.

e. **Reduces the amount of energy wasted:**
The amount of energy wasted is a function of the number of physical servers, as the number of physical servers get reduced then the amount of energy wasted also gets reduced.It helped to make cloud computing more efficient and ecofriendly.

IV. TYPES OF VIRTUAL MACHINE

A virtual machine (VM) is an abstraction layer or the environment between hardware components and the end-user. Virtual machines have an ability to run any operating systems on them and provide functionality of a physical computer

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

that are carefully separated by each other. They can be moved between several servers and computers. The interaction between the guest operating systems in virtual machines (VM's) and resources which are available for sharing between virtual machines, provided in two ways. One is by using the host operating system, or a piece of software which called as the hypervisor can run many virtual machines. Hypervisor is also known as virtual machine monitors (VMM). They are able to share system hardware components such as CPUs, controllers, disk, memory, and I/O among virtual servers.

Hypervisor

A hypervisor or virtual machine monitor (VMM) is a software that creates and runs virtual machines and it is also responsible for controlling, supervising, resource sharing and reallocating the virtual machines. It is an intermediate layer between operating system and hardware. A hypervisor runs one or more virtual machines on a machine which is called as host machine. Each of the virtual machine is called a guest machine. It also manages the execution of the guest OS. As the operating system number increases managing is difficult these leads to security issues. If a hacker gets control over the hypervisor he can control the guest systems by knowing the behavior of the system which causes data processing damage. Advanced protection system has been developed to monitor the activities of the guest OS. Hypervisor provides an isolated environment for VM's to achieve the secure environment for virtual machines, and it is also responsible for communication between VM's which usually called as virtual machines inter-VM communication. There are some approaches used for high speed inter-VM communication like Socket-Outsourcing , XenSockets ,Xway and XenLoop are using a simple shared memory channel for exchanging network packets. Basically, hypervisor is classified as bare metal hypervisor and hosted hypervisor. The bare metal hypervisor runs directly on the hardware whereas hosted hypervisor runs on the host operating system.

Type 1 (or) Bare Metal Hypervisor

Here the hypervisor is directly installed on the host hardware and then the virtual machines are installed on to the hypervisor. The virtual machines are also known as Guest Operating System.The operating system on which the hypervisor runs one or more virtual machines is called as Host Operating System. LynxSecure, RTS Hypervisor, Oracle VM, Sun xVM Server, VirtualLogic VLX are examples of Type 1 hypervisor.

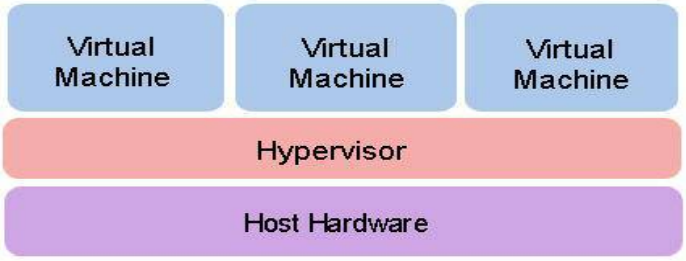

Figure 1: Bare metal Hypervisor

Type 2 (or) Hosted Hypervisor

Here firstly, Host Operating System is installed on the Host hardware and then the hypervisor is installed on Host Operating System and then the virtual machines are installed on to the hypervisor.Virtual Box, Windows Virtual PC and VMWare workstation 6.0 are examples of Type 2 hypervisor.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

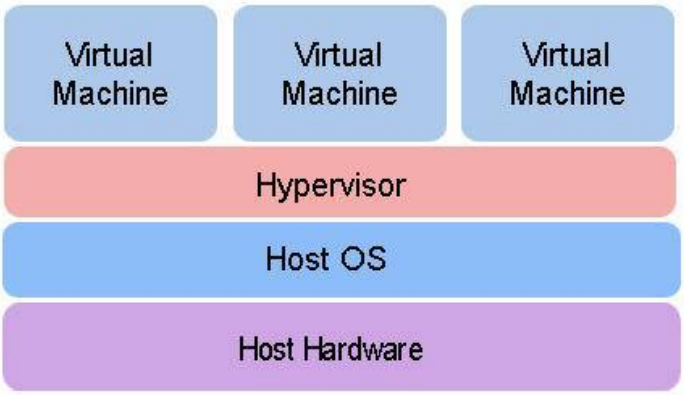

Figure 2: Hosted Hypervisor

Types of virtualization:

In cloud computing, there are three major types of virtualization such as Storage virtualization , Software virtualization and Server virtualization.

a. **Storage virtualization:**
The storage available is virtualized to get large virtual storage from physical storage. It is used for allocating memory to the clients. The significant point of the storage virtualization is to hide geographical(physical) locations of the data over the cloud environment. This is widely used in datacenters where you have a big storage and it helps you to create, delete, allocated storage to different hardware. This allocation is done through network connection.

b. **Software virtualization:**
For instance, software built by the company can be used by a large number of systems at the same time with the help of virtualization. A virtual layer is created on which the software is installed and used.

c. **Server virtualization:**
The server administrator uses a software application to divide one physical server into multiple isolated virtual servers, where you do not have to use any more physical servers for different purposes. Each virtual server may run the same or different operating systems. The advantages of virtualization include lower capital expenses, high availability and efficient use of resources.The significant point of the server virtualization is to increase the CPU utilization.

Advantages:

Without virtualization, cloud computing can be inefficient and difficult for the users. Virtualization is one of the cost-saving, energy-saving and hardware-reducing technique.

The virtualization provides

a. **Using Virtualization for Efficient Hardware Utilization:**
Virtualization decreases costs by reducing the need for physical hardware systems. Virtual machines use efficient hardware, which lowers the quantities of hardware, associated maintenance costs and reduces the power along with cooling the demand.

b. **Using Virtualization to Increase Availability:**
Virtualization platforms offer a number of advanced features that are not found on physical servers, which increase uptime and availability.

c. **Disaster Recovery:**
Disaster recovery is very easy when your servers are virtualized. With up-to-date snapshots of your virtual machines, you can quickly get back up and running.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

d. Save Energy:

Moving physical servers to virtual machines means lowering monthly power and cooling costs in the data center. It reduces carbon footprint and helps to clean up the air we breathe. Consumers want to see companies reducing their output of pollution and taking responsibility.

V. THE DYNAMIC VIRTUAL MACHINES IN CLOUD DATA CENTER

In order to dynamically provisioning resources for virtualized multi-tier application execution environments (VAEEs) of different customers, the most common approaches are based on self-managing techniques [9], such as Monitor, Analyze, Plan, and Execute (MAPE) control loops architecture is needed. The goal is to meet the virtualized application requirements while adapting IT architecture to workload variations. Usually, each request requires the execution of virtualized application allocated

on the VM of each physical tier. A cloud data center enables multiple virtualized applications may be increased when workload increases and reduced when workload reduces. This dynamic resource provision allows flexible response time in a VAEE where peak workload is much greater than the normal steady state. Figure 1 provides a high-level dynamic resource provision architecture for cloud data center, which shows relationships between computational resources pool and self-management community. **Computational Resources Pool** contains physical resources and virtualized resources. Plenty of VMs hold several VAEEs sharing the capacity of physical resources and can isolate multiple applications from the underlying hardware. VMs of each tier of a virtualized application may correspond to a physical machine. Computational resources pool delegates self-management community for satisfying the requirement goal of the customer to automatically allocate sufficient resources to the each tier of virtualized application. **Self-management community** means mechanisms to automate the VMs of configuring and tuning the virtualized multi-tier application so as to maintain the response time requirements of the different customers. It generates result of run-time provisioning for cloud data center. It includes four components as follows:

- **a. Monitor**: collects the workload and the performance metric of all running VAEEs, such as the request arrival rate, the average service time, and the CPU utilization, etc.
- **b. Analyzer**: receives and analyzes the measurements from the monitor to estimate the future workload. It also receives the response times of different customers.
- **c. Resource Scheduler**: sets up performance analytic models for each tier of the VAEE, and uses its optimizer with the optimization model to determine resource provisioning according to these workload estimates and response time constrains of different customer such that the resource requirements of the overall VAEE is minimized.
- **d. Virtualized application Executor**: assigns the VM configuration, and then runs the VAEEs to satisfy the resource requirements of the different customers according to the optimized decision. The goal is to minimize the using of resources under a workload while satisfying different customer for the constraints of average response time.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

S. No	Hypervisor Name	Company	Hypervisor Model	Virtualization Types			
				Full	Para	Hardware Assisted	Operating System
1	KVM	Red Hat	Hosted	Yes	No	No	No
2	XEN	Citrix systems, inc.	Bare Metal	No	Yes	Yes	No
3	VirtualBox	Oracle	Hosted	No	Yes	Yes	No
4	OpenVZ Linux	OpenVZ	Hosted	No	No	No	Yes
5	Linux-Vserver	Linux-Vserver	Hosted	No	No	No	Yes
6	Proxmox VE	Proxmox	Bare Metal	Yes	No	No	Yes

Table1: Comparison of open source hypervisor virtualization types

VI. FUTURE SCOPE AND CHALLENGES

The virtualization techniques get universal support when users consider elastic resource management issues and security issues before moving into cloud. In future, we aim to develop new policies, framework and techniques to maintain elastic resources and data availability, as a result, the performances of cloud services could steps into next higher level. Data loss, data security and inconvenience to access the data are some of the major problems that users face, so to solve all these problems, the major future aspects are:

a. Establishing Access control policies.
b. Using secure connections.
c. Implementing strong encrypting techniques.
d. Applying data loss prevention policies.
e. Checking client identities.
f. Enabling secure migration.
g. One user-many devices relationship
h. Problem of geographical distance between clients and servers can be avoided.

One of the major challenges in virtualization are:

a. Managing resources and Monitoring the data.
b. Running applications with high utilization and availability
c. If a virus infects into one file then it may corrupt the whole system.
d. The integrity of data can be affected as anyone can access it anytime and from anywhere.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

VII. CONCLUSION

This study paper discussed various virtualization types, hypervisor types and its challenges in cloud computing system to reduce IT costs and to increase the utilization of cloud resources. In addition, the virtualization techniques gets support when users first priority is to consider resource management issues and security issues in the cloud. In this paper cloud computing and virtualization has been briefly introduced. This contains the need, advantages and future scope of virtualization also.

REFERENCES

[1] Pearson S. Taking account of privacy when designing cloud computing services. In CLOUD '09: Proceedings of the 2009 ICSE workshop on software engineering challenges of cloud computing, IEEE Computer Society, Washington, DC, USA, 2009. pp. 44–52.
[2] Gu L, Cheung S-C. Constructing and testing privacy-aware services in a cloud computing environment: challenges and opportunities. In Internetware '09: Proceedings of the first Asia-Pacific symposium on internetware. ACM New York, NY, USA, 2009. pp. 1–10.
[3] Siebenlist F. Challenges and opportunities for virtualized security in the clouds. In SACMAT '09: Proceedings of the 14th ACM symposium on access control models and technologies, ACM, New York, NY, USA, 2009. p. 1–2.
[4] Cachin C, Keidar I, Shraer A. Trusting the cloud. SIGACT News 2009;40(2):81–6.
[5] Enisa. Cloudcomputingriskassessment. /http://www.enisa.europa.eu/act/rm/ files/deliverablesS, 2009.
[6] Armbrust M, Fox A, Griffith R. Above the clouds: A Berkeley view of cloud computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, February 2009.
[7] Ristenpart T, Tromert E, Shacham H, Savage S. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. In CCS '09: Proceedings of the 14th ACM conference on computer and communications security, ACM, New York, NY, USA, 2009. p. 103–15.
[8] Kim GH, Spafford EH.. The design and implementation of tripwire: a file system integrity checker. In CCS '94: Proceedings of the 2nd ACM conference on computer and communications security. ACM, New York, NY, USA, 1994. pp. 18–29.
[9] AIDEteam. Advanced intrusion detection environment/http://sourceforge.net/ projects /aideS, November2005.
[10] Secunia. Secuniaadvisory. /http://secunia.com/advisories/36389S, 2009.
[11] Jiang X, Wang X, Xu D. Stealthy malware detection through vmm-based ''out-of- the-box'' semantic view reconstruction. In CCS '07: Proceedings of the 14th ACM conference on computer and communications security. ACM, New York, NY, USA, 2007. pp. 128–38.
[12] Seshadri A, Luk M, Qu N, Perrig A. Secvisor: a tiny hypervisor to provide lifetime kernel code integrity for commodity oses. In SOSP '07: Proceedings of twenty- first ACM SIGOPS symposium on operating systems principles, ACM, New York, NY, USA, 2007. p. 335–50.
[13] Payne BD, Carbone M, Sharif M, Lee W. Lares: An architecture for secure active monitoring using virtualization. In SP '08: Proceedings of the 2008 IEEE symposium on security and privacy (sp 2008), IEEE Computer Society, Washington, DC, USA, 2008. pp. 233–47.
[14] Peter M, Schild H, Lackorzynski A, Warg A. Virtual machines jailed: virtualization in systems with small trusted computing bases. In VDTS '09: Proceedings of the 1st EuroSys Workshop on virtualization technology for dependable systems, ACM, New York, NY, USA, 2009. p. 18–23.
[15] Riley R, Jiang X, Xu D. Guest-transparent prevention of kernel rootkits with vmm- based memory shadowing. In RAID '08: Proceedings of the 11th international symposium on recent advances in intrusion detection, Springer-Verlag, Berlin, Heidelberg, 2008. p. 1–20.
[16] Rhee J, Riley R, Xu D, Jiang X. Defeating dynamic data kernel rootkit attacks via vmm-based guest-transparent monitoring. Availability, Reliability and Secur- ity, 2009. ARES '09. International Conference on, 2009.
[17] Lombardi F, Di Pietro R. A security management architecture for the protection of kernel virtual machines. In TSP '10: Proceedings of the Third IEEE international symposium on trust, security and privacy for emerging applications (to appear), IEEE Computer Society, Washington, DC, USA, 2010.
[18] Ranadive A, Gavrilovska A, Schwan K. Ibmon: monitoring vmm-bypass capable infiniband devices using memory introspection. In HPCVirt '09: Proceedings of the 3rd ACM workshop on system-level virtualization for high performance computing, ACM, New York, NY, USA, 2009. p. 25–32.
[19] Salza S, DiCarlo Y, Lombardi F, Puccinelli R. Leveraging the grid for the autonomic management of complex infrastructures. In: GCA grid computing and applications conference proceedings, 2006. p. 32–7.
[20] Huang Y, Arsenault D, Sood A. Closing cluster attack windows through server redundancy and rotations. In CCGRID, 2006. p. 21.
[21] Distler R, Kapitza R, Reiser HP. Efficient state transfer for hypervisor-based proactive recovery. InWRAITS '08: Proceedings of the 2nd workshop on recent advances on intrusiton-tolerant systems. ACM, New York, NY, USA, 2008. pp. 1–6.
[22] Sousa P, Bessani AN, Correia M, Neves NF, Verissimo P. Resilient intrusion tolerance through proactive and reactive recovery. Pacific Rim International Symposium on Dependable Computing, IEEE 2007;0:373–80.
[23] Pollitt M, Nance K, Hay B, Dodge RC, Craiger P, Burke P, Marberry C, Brubaker B. Virtualization and digital forensics: a research and education agenda. J. Digit. Forensic Pract. 2008;2(2):62–73.
[24] Haeberlen A. A case for the accountable cloud. In LADIS '09: 3rd ACM SIGOPS International workshop on large scale distributed systems and middleware, 2009.
[25] SP 800-57, Part 1, Recommendation for Key Management: General, July 2012.
[26] SP 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007.