International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 08 | Nov-2015 www.irjet.net p-ISSN: 2395-0072

Virtual Machine migration with secured Hypervisor-Based Technology

Debabrata Sarddar[1], Enakshmi Nandi[2]

[1] *Assistant Professor, Department Of Computer Science and Engineering, University Of Kalyani, West Bengal, India*
[2] *Ph.D student, Department Of Computer Science and Engineering, University Of Kalyani, West Bengal, India*

Abstract - ***Cloud Computing is one of the emerging and innovative technology now a day, which is familiar as scalable and elastic computing. It is also cost effective due to resource multiplexing, service provider is passed on to cloud users with lower cost and users can be paid only for the resources they used. Cloud computing is based on virtualization. Virtualization basically abstracts the fundamental resources and simplifies their use, separate clients from one another and supports replication which helps to enhances the elasticity of the system. But Virtualization maintained only limited security. So it creates a hindrance in the wide area environment like as cloud. In case of virtual migration process a virtual machine move from one host to another host instantly. It is a vital issue to maintain a robust security at the time of virtual machine migration.***

This paper proposes a new security based architecture in a hypervisor-based virtualization at the time of virtual machine migration to offer more elastic security against malicious attacks.

Key Words: Virtualization, hypervisor, security architecture, virtual machine migration, *etc…*

1. Introduction

Virtualization has activated a new generation of datacenters with more efficiency and availability for our most demanding workloads. Microsoft virtualization solutions better a performance on basic virtualization capabilities, such as consolidating server hardware, to develop comprehensive platforms for private and hybrid cloud [1]. In computing, virtualization means to develop a virtual version of a device or resource, such as a server, storage device, operating system or an network where the framework partition the resource into one or more execution environments. Virtualization can be defined as part of an complete trend in enterprise IT that belongs to an autonomic computing, a scenario in which the IT environment will be able to manage itself based on regarded activity, and utility computing, in which computer processing power is seen as a utility that users can pay for only as required. The main objective of virtualization is to centralize the administrative tasks while enhances scalability and workloads. The important benefits of virtualization is

a} Reduced Cost

b} Easier backup

c} No vendor-lock-in

d} Easier migration to cloud

e} Single minded server

f} Less heat buildup, etc.

Virtual Machine (VM) migration is a powerful management technique that provides data centre operators the ability to accustomed the placement of VMs in order to better fascinate performance objectives, improve resource utilization and communication locality, mitigate performance hotspots, getting fault tolerance, decrease the energy consumption, and facilitate system maintenance activities[2]. VM migration poses new necessities on the design of the underlying communication infrastructure, such as addressing and bandwidth requirements to support VM mobility. Furthermore, devising efficient VM migration schemes is also a challenging problem, as it not only needed the weighing advantages of VM migration, but also considering migration costs, including communication cost, service disruption, and management overhead. In this paper we layout a hypervisor based technology for improving the security issue of virtual machine migration process.

2. Types of Virtualization

Virtualization is a combination of software and hardware engineering that designs Virtual Machines (VMs) - an abstraction of the computer hardware that permits a single machine to act as if it where many machines. Virtualization mainly enables various operating systems to run on the same physical platform. Here physical server is called host and virtual machine servers are called guests.
There are three types of virtualization. Those are
i] Operating System-Based Virtualization
ii] Hypervisor based Virtualization
iii] Application based Virtualization

2.1 Operating System-based Virtualization

Operating system-based virtualization refers to the usage of software to allow system hardware to run various instances of different operating systems concurrently, permitting us to run different applications requiring for different operating systems on one computer system. Operating-system-level virtualization is mainly used in virtual hosting environments, where it is useful for securely allotting finite hardware resources amongst a large number of mutually-suspicious users. System administrators may use it, to a lesser extent, for consolidating server hardware by moving services on distinct hosts into containers on the one server [3].

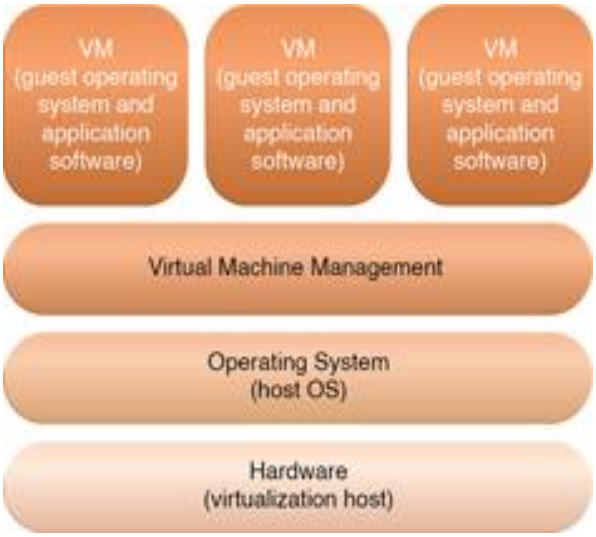


Fig1. Operating system-based Virtualization

2.2 Application-based Virtualization

Application virtualization is the separation of an installation of an application from the user computer that is accessing it. This virtualization is software technology that encases application software from the underlying operating system on which it is executed. The application behaves at runtime like it is directly interfacing with the original operating system and all the resources managed by it, but can be separated or sandboxed to varying degrees. There are two types of application virtualization: remote and streaming. With the help of application virtualization, each application reduces its own set of configurations on-demand [4], and executes in a way so that it sees only its own settings. This leaves the host operating system and existing settings unaltered.

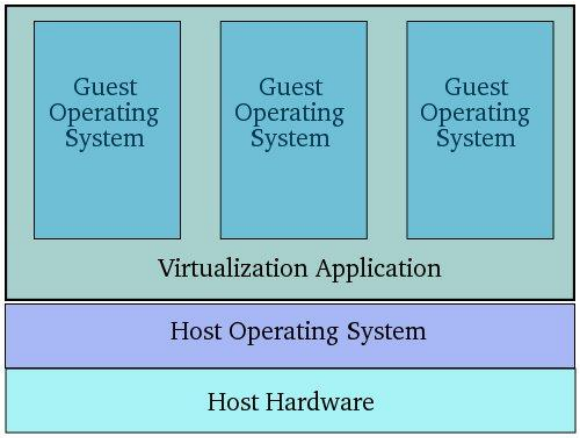


Fig 2: Application-based virtualization

2.3 Hypervisor-based Virtualization

hypervisor based virtualization is that, everything is done based on a hardware level, that is if the base operating system (the operating system on the physical server, which has hypervisor running), has to modify anything in the guest operating system (which is running on the virtual hardware created by the hypervisor), it can only modify the hardware resources [5], and nothing else. The basic idea behind this virtualization technique is that imitates the underlying physical hardware (with our desired resources like processor and memory) and on top of this newly developed virtual hardware an operating

system is installed. So this type of virtualization is basically operating system sceptics. Hypervisor controls the physical server's resources.

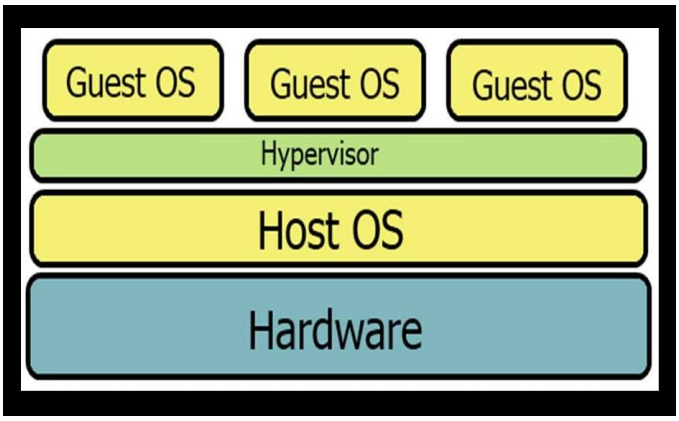


Fig3: Hypervisor-based Virtualization

3. Virtual Machine Migration

Virtual machine migration represents a new challenge to design efficient and practical migration algorithms that work well with hundreds or even thousands of VMs and servers [6]. Virtual Machine (VM) migration is a powerful management technique that provides data centre operators the ability to habituate the placement of VMs in order to better satisfy performance goals, improve resource utilization and communication locality, mitigate performance hotspots, won fault tolerance, bring down energy consumption, and facilitate system maintenance activities. As a VM primarily consumes four types of resources, those are, CPU, memory, disk and network resources, and the migration module is victim for migrating the state of each type of resource from the source to the destination machine [18]. In VM migration process, memory placement is divided into following phases [7].

i] Push Phase: In this phase source VM running simultaneously at the time of certain pages are pushed across the network to the new destination .Even pages which are moderated during migration must be resent for keep up consistency.

ii] Stop and copy phase: Here source VM is stopped, pages are copied across destination VM and new VM is started at that time. The time gap between VM staggering on source host and starting VM on destination host is called down time. This time relies on two factors; those are memory size and applications executing on VM [7].

iii] Pull Phase: Here new VM is created and initiate it execution, and if it accesses a page that has not still been copied, this page faulted in across the network from source VM. At VM migration the virtual machine at source are suspended, necessary CPU state, memory and registers are moved to the destination. The virtual machine resumed at destination but entire memory is not moved still then, less amount of data yet exit on source .In case when necessary page is not found on destination host, then page fault called network fault happens. Source machine make up that fault by sending the respective pages across the network.

4. Virtualization threats

In virtual environments, there are multiple attack outlets. Virtualization threats can enhances the security of cloud computing, by protecting both the integrity of guest virtual machines and the cloud infrastructure components [8]. With the help of hypervisor, all users see their systems as self-contained computers isolated from other users, even though every user is served by the same machine.

a) Virtual machine level attacks:
The hypervisor and/or virtual machines used by cloud vendors are a potential dilemma in multi-tenant architecture [9].

b) Cloud provider vulnerabilities:
These could be platform-level, such as an SQL-injection or cross-site scripting vulnerability that stay in cloud service layer which motive is insecure environment.

c) Expanded network attack surface:
The cloud client must conserve the infrastructure used to join client with the cloud; this task is intricate by the cloud if the firewall is abandoned: a scenario found in many cases.

d) Authentication and Authorization*:*

The enterprise authentication and authorization framework does not naturally prolong into the cloud. Enterprises have to combine cloud security policies with their own security metrics and policies.

e) Lock-in:
The cloud provider can encrypt user data in a specific format. If the client decides to migrate to another vendor with an incompatible format, this will appoint a problem on the client [10].

f) Data control in cloud:
Midsize businesses are used to have entire visibility and monitor over their entire IT portfolio. However, transferring some components into the cloud creates operational "blind spots", with little advance warning of degraded or interrupted service [11].

g) Communication in virtualization level:
Virtual machines have to communicate with each other. In some cases, they may need to share data. If these communications did not satisfy respective security parameters, then they are intending to attacks.

h) Virtualization Attacks:
Cloud gives services to legal clients, it can also services to users that have malicious purposes. A hacker can use a cloud to host a malicious application to attain its goal which may be a DoS attacks against the cloud itself, or targeting another user in the cloud.

i)Attack between VMs or between VMs and VMM: One of the primary advantages that virtualization brings is isolation. This advantage, if not carefully deployed becomes a threat to the environment. Week isolation or inappropriate access control policy owing to inter attack between VMs (virtual machines) or between VMs and VMM (virtual machine monitor) [12].

j) Client to client attacks: One malicious virtual machine could infect all virtual machines installed on the same physical server. This is the largest security risk in a virtualized environment [13].

k) Virtual machine controlled by Host Machine: The host controls all the network traffic going to or coming from the VMs through the host. So, if a host is attacked, then the security of the VMs is under question. Thus provision should be taken while configuring the VM environment in such a way to provide enough separation; this avoids the host being a gateway for attacking the virtual machine [12].

l) Denial of Service: A denial-of-service attacks (DoS attack) or distributed denial-of-service attack (DoS attack) is an attempt to make a computer resource unavailable to its respective clients. In virtual machine architecture, the guest machines and the underlying host share the physical resources such as CPU, memory, hard disk, and network resource. So it is possible for a guest to introduce a denial of service attack to other guests residing in the same system. Denial of service attack in a virtual environment can be defined as an attack when a guest machine takes all the possible resources of the system [12].

m) VM sprawl: VM sprawling is a case in which the number of VMs is continuously flourishing, while most of them are idle or never back from sleep. This is responsible for a vast wastage of the host machine's resources [12].

5. Related work

Elmroth et al. [14] have discovered technology neutral interfaces and architectural additions for performing placement, migration, and controlling of VMs in federated cloud environments, the next part is an extension of current monitoring architectures used in grid computing. The interfaces presented connected to the general necessities of scalability, efficiency, and security in addition to particular necessities related to the specific issues of interoperability and business relationships between competing cloud computing infrastructure providers. In addition, they may be used equally well locally and remotely, developing a layer of abstraction that simplifies management of virtualized service components. Beloglazov et al. [15] have defined a method for dynamic consolidation of VMs based on adaptive utilization thresholds, which decides a high level of reaching the SLA (Service Level Agreements).They validate the high efficiency of the proposed technique across several kinds of workloads using workload traces from more than a thousand Planet Lab servers. Dynamic consolidation of virtual machines (VMs) and switching idle nodes off permit Cloud providers to amend resource usage and decrease energy consumption. Beloglazov et al. [16] have discovered an adequate resource management policy for virtualized Cloud data centres. The main goal is to continuously consolidate VMs leveraging live migration and switch off idle nodes to underrate power consumption, while providing required Quality of Service.

6. Proposed Method

Here we think about the security issue during virtual machine migration . A lot of states moves over network channels during migration process which are often insecure .Even any hacker may create duplicate VM at the time of migration.In that case protecting contents of VM state files and maintain original VM as intact and protecting them from intruders is an critical issue. When data are transferred from source to destination host,if we create an hypervisor based technology at source host and starting the migration process ,then VM migration process will be more secured .Original VM migration process shows in following diagram.

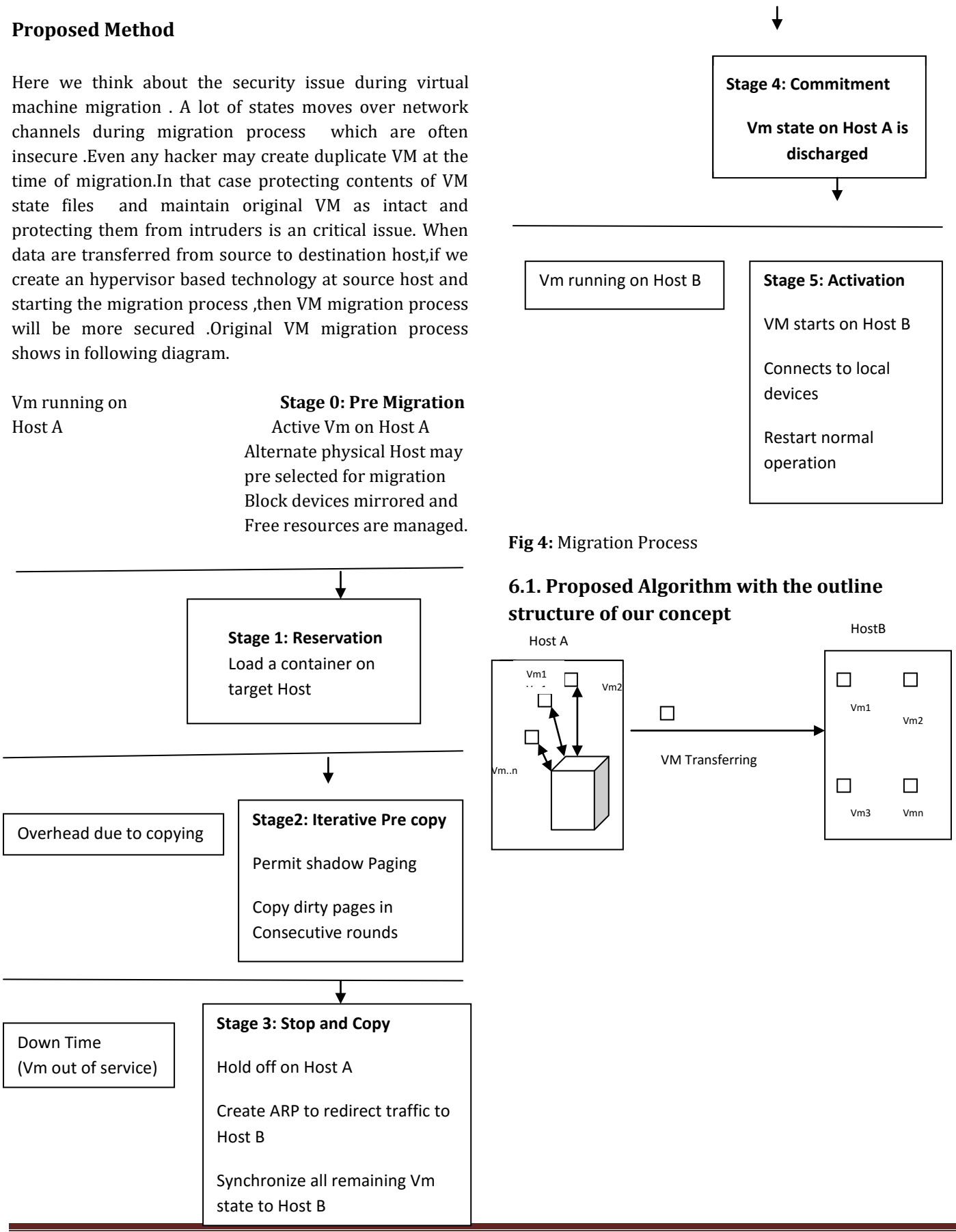
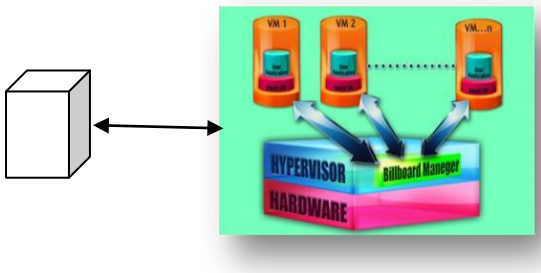


Fig 4: Migration Process

6.1. Proposed Algorithm with the outline structure of our concept



Billboard Manager based hypervisor

Fig 5: VM migration process with the help of Billboard manager based hypervisor

Step1: Active VM on host A and alternate physical host are preselected,load container on target host.

Step 2: Turning on the Billboard Manager based hypervisor technology on host A.

Step 3: Billboard Manager first stores all information about all virtual machines in hostA.All VM sends bacon signal to Billboard Manager(BM) and BM stroes all information like MAC address ,IP address,Operating system,all files and memory data values of all virtual machines.

Step 4: All VM sends information to Billboard Manager periodically.

Step 5*:* 3 If needed in shortest time within the bacon signal time, we forcefully scan (active scan) the Billboard Manager table.

Step 6: If false information about any VM node or duplicate VM is created by the hacker then that information came to BM and BM forcefully stop the working principal of false VM (which is created by hacker or by any criminal)

Step 7*:* If an administrator creates a new VM in host A that information also sent to the Billboard Manager for future record.

Step 8:Pre-copy state will start iteratively now and copy dirty pages in consecutive rounds.

Step9: Initiate start and copy state, hold off VM on host A, create ARP to redirect traffic to Host B and synchronize all remaining VM state to Host B.

Step 10: VM state is discharged on Host A, VM is running on host B, Connects to local devices, migration process is terminated.

3. CONCLUSIONS AND FUTURE WORK

Our object is to develop a secured VM migration technique to protect VM against unwanted intrusions. Our hypervisor based architecture provides that security with the help of Billboard manager which would be configured in a manner wherein even administrators of the hypervisor would have to register requests with the Billboard Manager for installation and access of virtual machines. Malicious attacks of planting ghost virtual machines can be thus pushed away as the Billboard Manager would reject for granting access to the hypervisor in case identities and digital signatures are not found in its own encrypted database[17]. So we can said that Billboard Manager introduce vigorous security at the time of VM migration process by ensuring that data flow is controlled at each turn within the cloud computing hypervisor architecture to which it is configured.

In future we will design more robust secured and first processing VM migration process for increasing efficiency and integrity of migration process.

REFERENCES

[1] file:///Virtualization for your modern datacenter and hybrid cloud Microsoft.htm

[2] file:///Virtualization with Cloud Computing For Dummies.htm

[3] https://en.wikipedia.org/wiki/Operating-system-level_virtualization

[4] http://www.webopedia.com/TERM/A/application_virtualization.html

[5]http://www.slashroot.in/difference-between-hypervisor-virtualization-and-container-virtualization

[6] Singh, Amritpal, and Supriya Kinger. "Virtual machine migration policies in clouds." *International Journal of Science and Research (IJSR)* 2.5 (2013): 364-367.

[7] "Virtual Machine Migration in Cloud Datacenters" by Jaspreet Kaur, Manpreet Kaur, Sahil Vashist, International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 8, August 2014 ISSN: 2277 128X

[8] Lombardi, F., Di Pietro, R.: Secure virtualization for cloud computing. Journal of Network and Computer Applications, 34(4), (2011).
[9] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., Molina, J.: Controlling Data in the Cloud: Outsourcing Computation Without Outsourcing Control. In Proceedings of the 2009 ACM workshop on Cloud Computing Security, (2009).
[10] Sefton, P.: Privacy and Data Control in the Era of Cloud Computing. Brightline Lawyers, (2010).
[11] Rowe, D.: The Impact of Cloud on Mid-size Businesses.[Online].
Available:http://www.macquarietelecom.com/hosting/blog/cloud-computing/im, (2011).
[12]Luo, S., Lin, Z., Chen, X., Yang, Z., Chen, J.: Virtualization security for cloud computing service. In IEEE International Conference for Cloud and Service Computing (CSC), (2011).
[13] Sabahi, F.: Secure Virtualization for Cloud Environment Using Hypervisor-based Technology. Int. Journal of Machine Learning and Computing, 2(1), (2012).
[14]Beloglazov and R. Buyya, "Energy Efficient Allocation of Virtual Machines in Cloud Data Centres," 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, May 2010, pp.577-578, 2010.
[15] W. Voorsluys, J. Broberg, S. Venugopal, and R. Buyya, "Cost of Virtual Machine Live Migration in Clouds: A Performance Evaluation," 1st International Conference on Cloud Computing, pp. 254-265, 2009.
[16] J. Sonnek, J. Greensky, R. Reutiman and A. Chandra, "Starling: Minimizing communication overhead in virtualized computing platforms using decentralized affinity-aware migration," 39th International Conference on Parallel Processing (ICPP) Sep 2010,
pp. 228-237, 2010.
[17] Bose, Rajesh, and Debabrata Sarddar. "A Secure Hypervisor-based Technology Create a Secure Cloud Environment." (2014).
[18] Debabrat Sarddar,Enakshmi Nandi."Efficient virtual machine migration with reduced migration time and downtime"(2015).

BIOGRAPHIES

Debabrata Sarddar is an Assistant Professor at the Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, India. He completed his PhD from Jadavpur University. He did his M. Tech in Computer Science & Engineering from DAVV, Indore in 2006, and his B.E in Computer Science & Engineering from NIT, Durgapur in 2001. He has published more than 75 research papers in different journals and conferences.His research interests include Wireless and Mobile Systems and WSN, and Cloud computing.

Enakshmi Nandi received her M.Tech in VLSI andMicroelectronics from Techno India, Salt Lake, West Bengal and B.Tech in Electronics and Communication
Engineering from JIS College Of Engineering, West Bengal under West Bengal University of Technology, West Bengal, India. At present, she is Research scholar in Computer Science and Engineering from University of Kalyani. Her research interests include Cloud Computing, Mobile Communication system, Device and Nanotechnology.