International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-2)

Research Article | **February 2015**

A Secure Hypervisor-based Technology Create a Secure Cloud Environment

Rajesh Bose, Debabrata Sarddar
Department of Computer Science & Engineering University of Kalyani
Nadia, West Bengal, India

Abstract:

As one of the most exciting technologies which have matured in the world today, Cloud Computing has emerged as one which has garnered the most appeal as being flexible and scalable. It has been known to reduce both complexity as well as cost of applications. What was once a dream has now manifested itself as a reality embraced by leaders not only in the industry but in research institutions and various organizations in multitude of spheres? Cloud computing is based on virtualization, A technology in itself which is not quite new. However, the security issues which followed virtualization now poses an equal challenge in case of cloud computing. Further, virtualization can offer only limited security capabilities. This, therefore, poses a significant hurdle which needs to be surmounted in order to secure a wide area environment such as the cloud. The development of a resilient and sturdy security system demands that changes be made derived from traditional virtualization architecture. This paper proposes new security architecture in a hypervisor-based virtualization with the sole objective to offer security against malicious attacks.

Key words - cloud computing, virtualization, security architecture, hypervisor.

I. INTRODUCTION

There have been various waves of technology that have swept the base of IT in the current scenario but the one technology that has made a mark in the IT and as well as corporate in sector Virtualization. In recent, many IT users won't have powerful machines but they are interested in powerful IT services. The answer to this demand lies with application virtualization using cloud computing and virtualization technologies [1, 2, 3]. It is a technique for hiding the physical characteristics of computing resources to simplify the way in which other systems, applications, or end users interact with those resources. Virtualization is very important for cloud computing and as a result brings another benefit that cloud computing is famous for, scalability. Because each virtual server is allocated only enough computing power and storage capacity that the client needs, more virtual servers can be created. But if the needs grow, more power and capacity can be allocated to that server, or lowered if needed. And because clients only pay for how much computing power and capacity they are using, this can be very affordable for most clients. Without virtualization, cloud computing as we know it would not exist or would be in a different form. But such is now only in the realm of speculation as virtualization is really here to make Information Technology more affordable for the world. Virtualization becomes an innovative software usage model that has many benefits as follows.

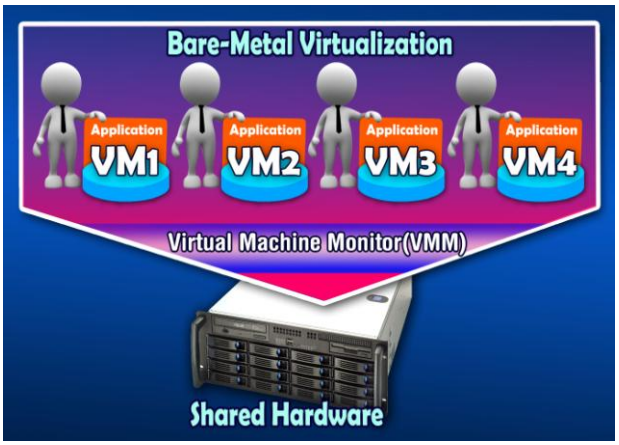
- Cost reduction
- Better hardware utilization
- Centralized management
- Minimizing outage during maintenance
- Faster deployment of new applications.

In rest of the paper is organized as follows, in section II we discuss the Virtualization and its types, in section III we discuss threats and attacks in virtualization, in section IV we discuss here related work and in section V we introduce our proposed worked. Section VI contains the proposed algorithm, Section VII contain flowchart and in section VIII we discuss the conclusion part of the paper.

II. VIRTUALIZATION AND ITS TYPES

Virtualization is an abstraction layer that's breaks the hard connection between the physical hardware and the operating system. A virtual infrastructure is an enterprise wide solution that provides fluid, powerful computing that maximizes resource utilization and cost savings. Virtual machines are the key element to a virtual infrastructure. Virtualization allows us to run multiple virtual machines with heterogeneous operating systems and application to run in isolation, side-by-side on the same physical machine.

There are three types of virtualization: Operating System-Based Virtualization, Hypervisor-Based Virtualization and Application-Based Virtualization. They all share a few common traits. The physical server is called the host. The virtual servers are called guests. The virtual servers behave like physical machines. Each system uses a different approach to allocate physical server resources to virtual server needs. The architecture of these approaches is started



(a) Operating system-based Virtualization

(b) Application-based Virtualization

(c) Hypervisor-based Virtualization

Fig1.Virtualization approaches [11]

A. Operating System-Based Virtualization:

In this approach (Fig 1.a), virtualization is enabled by a host operating system that supports multiple isolated and virtualized guest OS's on a single physical server [4]. The biggest limitation of this approach is that all the guest servers must run the same OS. Each virtual server remains independent from all the others, but you can't mix and match operating systems among them. Because all the guest operating systems must be the same, this is called a homogeneous environment.

B. Hypervisor-Based Virtualization:

In this approach (Fig 1.c), The hypervisor interacts directly with the physical server's CPU and disk space. It serves as a platform for the virtual servers' operating systems. The hypervisor keeps each virtual server completely independent and unaware of the other virtual servers running on the physical machine. Each guest server runs on its own OS -- you can even have one guest running on Linux and another on Windows. The hypervisor monitors the physical server's resources. As virtual servers run applications, the hypervisor relays resources from the physical machine to the appropriate virtual server. Hypervisors have their own processing need, which means that the physical server must reserve some processing power and resources to run the hypervisor application. This can impact overall server performance and slow down applications.

C. Application-Based Virtualization:

An application-based virtualization is hosted on top of the hosting operating system (Fig 1.b). This virtualization application then emulates each VM containing its own guest operating system and related applications. This virtualization architecture is not commonly used in commercial environments. Security issues of this approach are similar to Operating system-based [4].

III. THREATS AND ATTACKS IN VIRTUALIZATION

Virtualization Threats - It can increase the security of cloud computing, by protecting both the integrity of guest virtual machines and the cloud infrastructure components [5]. With the hypervisor, all users see their systems as self-contained computers isolated from other users, even though every user is served by the same machine. In this context, a Virtual Machine is an operating system that is managed by an underlying control program.

a) *Virtual machine level attacks*:

The hypervisor and/or virtual machines used by cloud vendors are a potential problem in multi-tenant architecture [6].

b) *Cloud provider vulnerabilities***:**

These could be platform-level, such as an SQL-injection or cross-site scripting vulnerability that exist in cloud service layer which cause insecure environment.

c) *Expanded network attack surface:*

The cloud user must protect the infrastructure used to connect him with the cloud; this task is complicated by the cloud if the firewall is abandoned: a scenario found in many cases [6].

d) *Authentication and Authorization:*

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

e) *Lock-in:*

The cloud provider can encrypt user data in a particular format. If the user decides to migrate to another vendor with an incompatible format, this will impose a problem on the user [7].

f) *Data control in cloud:*

Midsize businesses are used to have complete visibility and control over their entire IT portfolio. However, moving some components into the cloud creates operational "blind spots", with little advance warning of degraded or interrupted service [8].

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 didn't meet significant security parameters, then they are subject to attacks.

h) *Virtualization Attacks:*

Basically, as the cloud gives services to legal users, it can also services to users that have malicious purposes. A hacker can use a cloud to host a malicious application to achieve his object which may be a DDoS attacks against the cloud itself, or targeting another user in the cloud. For example, an attacker knew that his victim is using a cloud vendor with name X, now attacker by using similar cloud provider can sketch an attack against his victim(s). This situation is similar to this scenario that both attacker and victim are in the same network, but with the difference that they use virtual machines instead of physical network (Fig 2) [7].

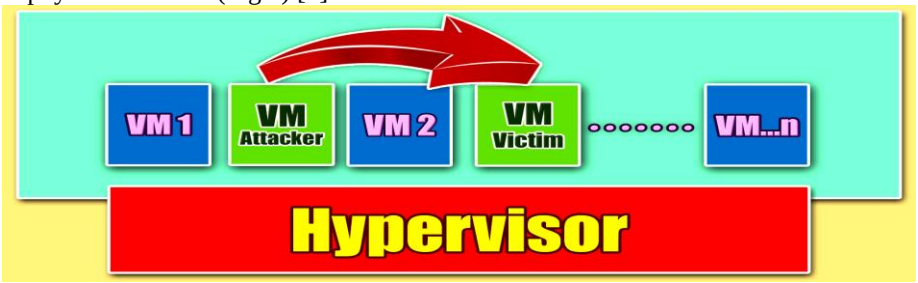


Fig 2. Attack scenario within cloud

i) *Attack between VMs or between VMs and VMM:*

One of the primary benefits that virtualization brings is isolation. This benefit, if not carefully deployed becomes a threat to the environment. Poor isolation or inappropriate access control policy causes the inter-attack between VMs (virtual machines) or between VMs and VMM (virtual machine monitor) [9].

j) *Client to client attacks:*

One malicious virtual machine could infect all virtual machines installed on the same physical server. This is the biggest security risk in a virtualized environment [4].

k) *Virtual machine controlled by Host Machine:*

The host monitors all the network traffic going to/coming from the VMs through the host. Therefore, if a host is attacked, then the security of the VMs is under question. Hence precautions should be taken while configuring the VM environment in such a way to provide enough isolation; this avoids the host being a gateway for attacking the virtual machine [9].

l) *Denial of Service:*

A denial-of-service attacks (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. 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 impose a denial of service attack to other guests residing in the same system. Denial of service attack in a virtual environment can be described as an attack when a guest machine takes all the possible resources of the system [9].

m) *VM sprawl:*

VM sprawling is a case in which the number of VMs is continuously growing, while most of them are idle or never back from sleep. This causes a large waste of the host machine's resources [9].

IV. RELATED WORK

A lots of research has been done in the field of secure virtualized environment in cloud computing. Here are some of them-

In [10] discussed a problem that current cloud computing services suffer from. More explicitly, this is the inability of isolating the computing resources and network between customers. This implies that data packets may share the same LAN. Such lack of isolation brings security risks to the users. Moreover, the scalability limitations of prior VLANs-based solutions do not allow the users to customize security policy settings the same way they control their on-site network. Therefore, an architecture that uses network virtualization as the main component for the security is suggested.

In [5], the authors proposed security architecture to protect the cloud based. The idea is based on virtualization; it is called Advanced Cloud Protection System (ACPS). It consists of a monitor key kernel or middleware component that is able to detect any modification to the kernel data and code. It also checks the behavior and the integrity of cloud components via logging and periodic checksum verification of executable files and libraries to manage monitoring cloud entry points. The system is implemented using open source code Open ECP and Eucalyptus.

In [4], the authors proposed virtualization architecture to secure cloud. In the proposed architecture, authors try to reduce the workload, decentralize security-related tasks between hypervisor and VMs, and convert the centralized security system to a distributed one. The distributed security system is a very good way to reduce the workload from hypervisor-based virtualization, but this distribution may inject vulnerabilities to cloud. In addition, distributed security systems have more complexity than centralized ones. Because of several benefits, such as the fault-tolerant capability, of distributed security management, it is not possible to ignore it and persist on centralized managing, but it is important to use a distributed management unit with care warily.

V. PROPOSED WORK

In a traditional model, a hypervisor supports a set of virtual machines each uniquely identified and setup by the usual administrator-run processes. Regardless of administrator privileges or permissions, malicious hackers can implant a ghost virtual machine to run in sync with the genuine virtual machines. In this way, hackers are able to glean vital data and information from the network as the hypervisor or its administrators would have no inkling as to the existence of this ghost virtual machine. This is an all too real unacceptable security breach and one which has the potential to lie undetected. In this paper, we added some features to virtualization architecture in order to improve security for cloud environment. Therefore, in the architecture, I included additional unit like Billboard Manager for monitoring the events and activities in VMs. Billboard Manager can prevent the attack, such as duplicate VM issue, that is created by an attacker or hacker but not in the BM list, that VM must be treated as a victim and then and there this type of vm must be deleted by BM automatically.Fig3 shows the Billboard Manager based hypervisor system.

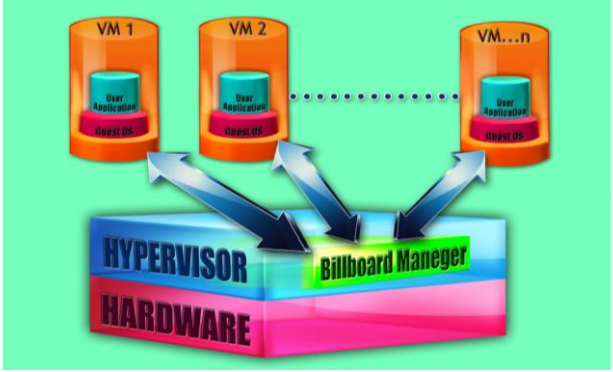


Fig3. Billboard Manager based hypervisor.

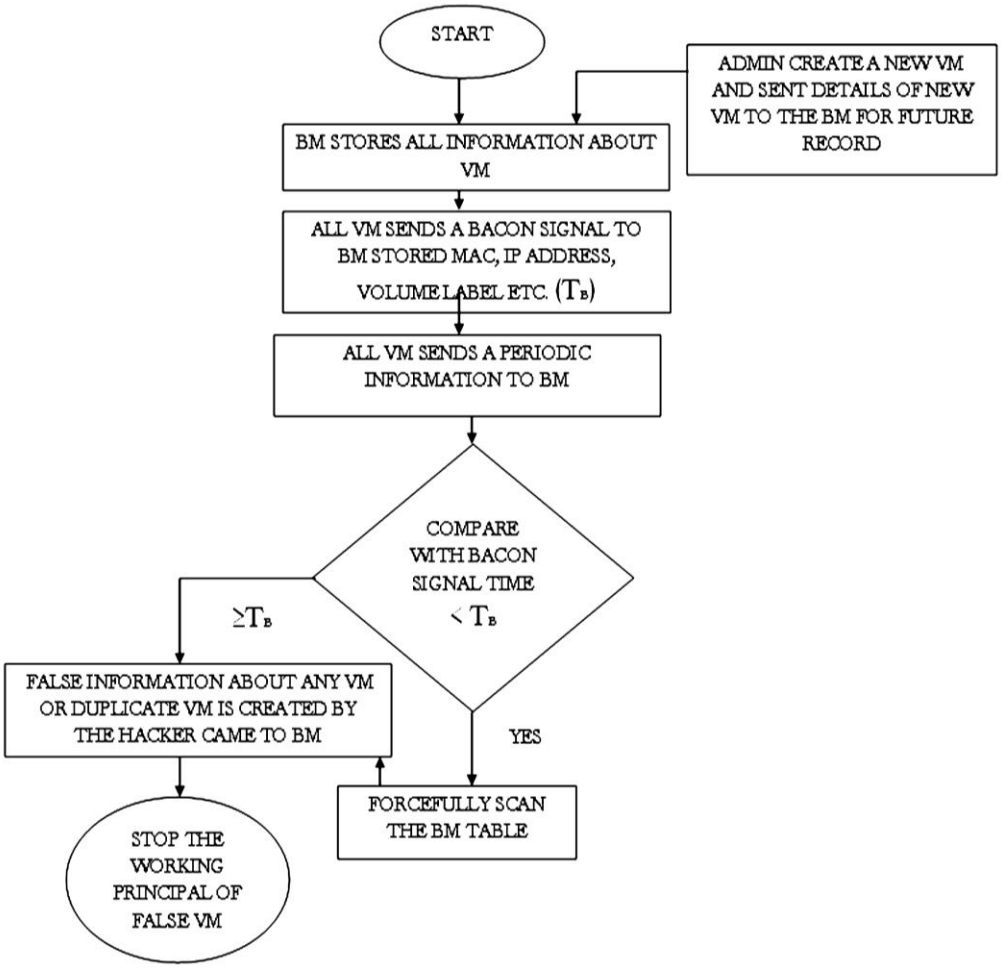
VI. ALGORITHM

Billboard Manager follows this algorithm

1. Billboard Manager stores all the information about the virtual machines, All VM sends a bacon signal to Billboard Manager to stores the information like MAC address, Volume label, IP address and Operating system.
2. All VM sends periodic information to Billboard Manager.
3. 3 If needed in shortest time within the bacon signal time, we forcefully scan (active scan) the Billboard Manager table.

4. If false information about any VM node or duplicate VM is created by the hacker that information came to BM and BM forcefully stop the working principal of false VM (which is created by hacker or by any criminal)
5. If an administrator create a new VM that information also sent to the Billboard Manager for future record

VII. FLOW CHART



VIII. CONCLUSION

The purpose of the paper is to introduce a new hypervisor-based architecture wherein the Billboard Manager is able to detect such unwanted intrusions. The Billboard Manager 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 repelled as the Billboard Manager would refuse granting access to the hypervisor in case identities and digital signatures are not found in its own encrypted database. The Billboard Manager is expected to introduce robust security to cloud computing by ensuring that data flow is monitored at every turn within the cloud computing hypervisor architecture to which it is configured.

REFERENCES

[1] C. W. Yoon, M. M. Hassan, H. W. Lee, et. al., "Dynamic Collaborative Cloud Service Platform: Opportunities and Challenges", ETRI Journal, vol. 32, no.4, **(2010)**, pp. 634–637.
[2] J. Gaudiosi, "Future of Cloud Gaming: Industry Leaders' Thoughts", FC Business intelligence, **(2011)**.
[3] K. Hwang, G. Fox and J. Dongarra, "Distributed and Cloud Computing: from Parallel Processing to the Internet of Things", Morgan Kauffman Publishers, **(2011)**.
[4] Sabahi, F.: Secure Virtualization for Cloud Environment Using Hypervisor-based Technology. Int. Journal of Machine Learning and Computing, 2(1), (2012).
[5] Lombardi, F., Di Pietro, R.: Secure virtualization for cloud computing. Journal of Network and Computer Applications, 34(4), (2011).
[6] 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).
[7] Sefton, P.: Privacy and Data Control in the Era of Cloud Computing. Brightline Lawyers, (2010).
[8] Rowe, D.: The Impact of Cloud on Mid-size Businesses.[Online].Available:http://www.macquarietelecom.com/hosting/blog/cloud-computing/im, (2011).

[9] 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).

[10] Hao, F., Lakshman, T., Mukherjee, S., Song, H.: Secure Cloud Computing with a Virtualized Network Infrastructure. In Proceedings of the 2 nd USENIX Conference on Hot Topics in Cloud Computing (HotCloud'10), (2010).

[11] Debabrata Sarddar and Rajesh Bose ,Architecture of Server Virtualization Technique Based on VMware ESXI server in the Private Cloud for an Organization,International Journal of Innovation and Scientific Research, ISSN 2351-8014 Vol. 12 No. 1 Nov. 2014, pp. 284-294

AUTHORS

Rajesh Bose is currently pursuing PhD from Kalyani University. He is an IT professional employed as Senior Project Engineer with Simplex Infrastructures Limited, Data Center, Kolkata. He received his degree in M.Tech. in Mobile Communication and Networking from WBUT in 2007. He received his degree in B.E. in Computer Science and Engineering from BPUT in 2004. He has also several global certifications under his belt. These are CCNA, CCNP-BCRAN, and CCA(Citrix Certified Administrator for Citrix Access Gateway 9 Enterprise Edition),CCA(Citrix Certified Administrator for Citrix Xen App 5 for Windows Server 2008).His research interests include cloud computing, wireless communication and networking.

Debabrata Sarddar, Assistant Professor in the Department of Computer Science and Engineering, University of Kalyani, Kalyani, Nadia, West Bengal, INDIA. He has done PhD at Jadavpur University. He completed 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 interest includes wireless and mobile system and Cloud computing.

