International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 12 No. 1 Nov. 2014, pp. 284-294

http://www.ijisr.issr-journals.org/

Architecture of Server Virtualization Technique Based on VMware ESXI server in the Private Cloud for an Organization

Debabrata Sarddar[1] and Rajesh Bose[2]

[1]Department of Computer Science & Engineering, University of Kalyani,
Nadia, West Bengal, India

[2]Simplex Infrastructures Ltd.
Data center, Kolkata, India

ABSTRACT: The recurring theme of server virtualization being a bundled single virtual machine file – consisting of the operating system, applications and settings – easily stored, deployable or transportable within the bounds of its operating parameters, the Achilles heel of such a VM (virtual machine) file is the likelihood of its getting corrupt or irrecoverably lost. Such disastrous occurrences are not unheard of, and are regularly tackled using a system of data backups to extenuate loss or corruption of entire VM files. However, the backing up process of VM files itself can compound recurring costs at an unexpected rate in the form of frequent acquisition of storage hardware in which to store the VM files. In this paper first we shows, a detailed cost comparison that based on power and cooling has been drawn in a table format between physical server and VMware server [VMware esx], secondly we analyze the role that the Billboard Manager has to play in shuttling the VM files in a secure and encrypted manner so as to extract the maximum operating potential of server virtualization and virtualization storage system in a private cloud domain.

KEYWORDS: virtual machine, operating system, storage, Billboard Manager, VMware, virtualization, private cloud.

1 INTRODUCTION

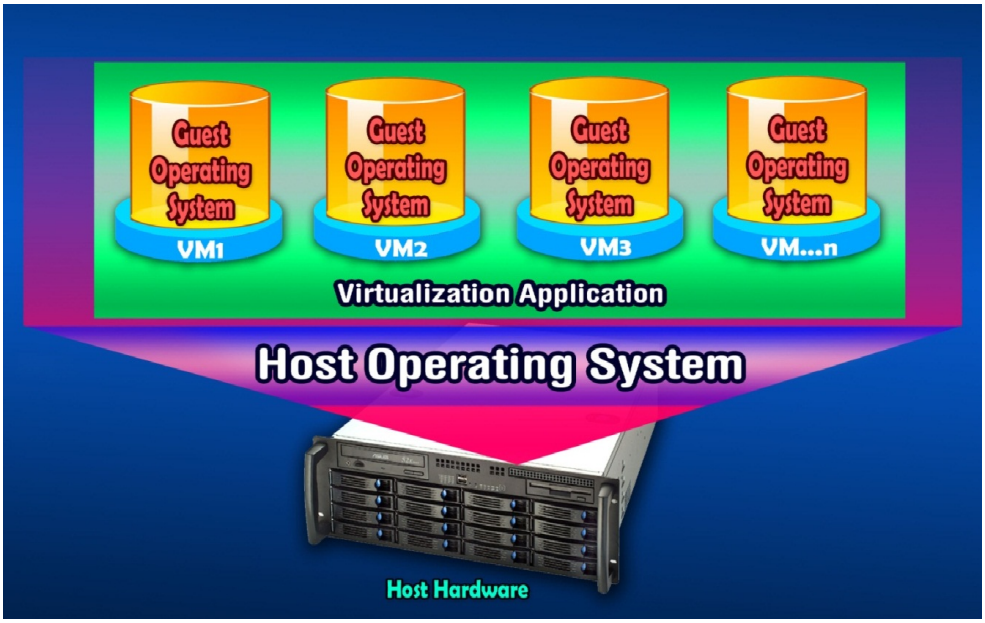
Virtualization is a core enabling technology of the Scalable Enterprise. Simply put, virtualization decouples software from hardware and presents a logical view of physical hardware to software. In other words, a single server can act and behave as multiple, independent servers. Virtualization and cloud computing are key features of any advanced agency infrastructure and, if done right, will reduce complexity and cost while improving the delivery of applications and services to the end user. The main purpose of using virtualization technology is to consolidate workloads so that one physical machine can be multiplexed for many different users. This improves the efficiency of an overall data center by allowing more work to be done on a smaller set of physical nodes [1], and also improves the per-server energy efficiency because even idle servers consume a great deal of energy [2]. In this paper, we focus on the server virtualization, and a proposed model that help us to encrypt and store all VM in a suitable storage area place. A virtual server is a logical representation of physical server in software. With server virtualization techniques, you can construct a virtual computing environment with multiple virtual machines on even a single Physical server, in which all virtual machines with varied environments share the same and flexibly configure various environments while simultaneously isolating the impact from malfunctioning user-software [3]. For example, we can install different operating systems like Linux, Window and UNIX, into individual virtual machines hosted in the same physical server. In this way, applications developed in varied environments can be run on a single physical server, leading to great flexibility of server configuration. Server virtualization is generally involved with server consolidation and cluster, which aims at making the management of massive datacenter environments substantially easier [4]. With the rapid growth of data stream, large computational clusters are deployed in many companies, which lead to heavy burden of management and instability of systems. For example, hundreds of global data centers suffer from severe interruption of services every year

Corresponding Author: Rajesh Bose

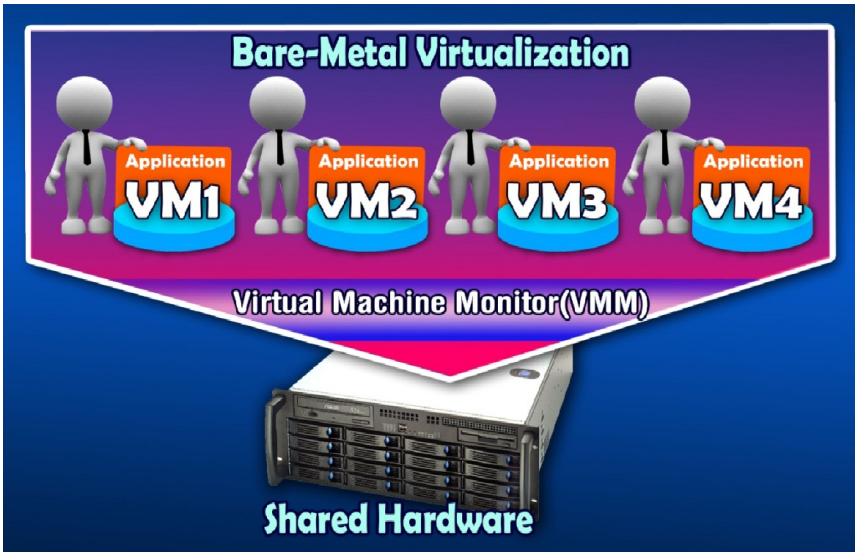
due to mistake operations of users, viruses, hardware failures, and natural disasters. Therefore, simplifying the datacenter management and fully utilizing the computing capability of large computational clusters become main issue in both industry growth and research. Employing server virtualization as computing environments provides a promising solution to these challenges, which allows administrators to more flexibly and accurately allocate the computing resources. While virtualization provides many conveniences, it comes at a cost. The hypervisor which manages the virtualization platform incurs some overhead simply because of the layer of abstraction it must add between a VM and the physical resources it makes use of [5]. Further, since many VMs may run on one physical machine, performance isolation is critical to ensure that competing VMs do not negatively impact one another. For example, a CPU scheduler in the hypervisor must provide a fair amount of time to each VM and prevent a greedy VM from hurting others [6, 7].The choice of hypervisor does not only apply to an enterprise's private data center—different cloud services make use of different virtualization platforms. Amazon EC2, the largest infrastructure cloud, uses Xen as a hypervisor, but Microsoft Azure uses Hyper-V and VMware partners use ESX. Recently, Google launched its own IaaS cloud that uses KVM as a hypervisor [8]. The rest of the paper is organized as follows. Section 2 provides virtualization approaches, Section 3 describe the Advantages of Virtualization Section 4 describes the VMware workstation. In Section 5, Describe about the encrypted data storage analysis, in Section 6, describes related work, in Section 7 describe the proposed work and Section 8` concludes the paper.

2 VIRTUALIZATION APPROACHES

In a traditional environment consisting of physical servers connected by a physical switch, IT organizations can get detailed management information about the traffic that goes between the servers from that switch. Unfortunately, that level of information management is not typically provided from a virtual switch. Basically, the virtual switch has links from the physical switch via the physical NIC that attaches to Virtual Machines. The resulting lack of oversight of the traffic flows between and among the Virtual Machines on the same physical level affects security and performance surveying. There are several common approaches to virtualization with differences between how each controls the virtual machines. The architecture of these approaches is illustrated in Figure 1



(a) Operating system-based Virtualization



(b) Application-based Virtualization

(c) Hypervisor-based Virtualization

Fig. 1. Virtualization Approaches

2.1 OPERATING SYSTEM-BASED VIRTUALIZATION

In this approach (Figure 1.a), virtualization is enabled by a host operating system that supports multiple isolated and virtualized guest OS's on a single physical server with the characteristic that all are on the same operating system kernel with exclusive control over the hardware infrastructure. The host operating system can view and has control over the Virtual Machines. There are several weaknesses for this architecture. One of main weaknesses is the performance degradation. When a virtual machine performs I/O operations from guest operating system, all these operations must be interpreted by the host operating system before arriving to hardware. This will increase extra CPU overhead and lead to performance degradation.

2.2 APPLICATION-BASED VIRTUALIZATION

An application-based virtualization is hosted on top of the hosting operating system (Figure1.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.

2.3 HYPERVISOR-BASED VIRTUALIZATION

A hypervisor is one of many virtualization techniques which allow multiple operating systems, termed guests, to run concurrently on a host computer, a feature called hardware virtualization. It is so named because it is conceptually one level higher than a supervisor. The hypervisor presents to the guest operating systems a virtual operating platform and monitors the execution of the guest OS (guest operating systems). Multiple instances of a variety of operating systems may share the virtualized hardware resources. Hypervisor is installed on server hardware whose only task is to run guest operating systems. Unlike the hosted architecture in which the virtual machines are installed within the hosted operating system, a virtual machine in bare metal architecture is installed directly on hardware. The virtualization layer directly controls the hardware and manages guest operating systems. Successive commercial software's following this architecture includes VMware ESXi, Citrix Xen Server and Microsoft Hyper-V. Since the bare metal model directly implements the virtualization in the hardware level, the system overhead transferring operation signal from guest operating system to the hardware is less than the hosted model. In addition, since the size of basis management software is very small (generally, 32M), the resource used by the virtualization layer can be ignored. Moreover, since the virtual machines are not built within a host operating system, the probability of malfunction is significantly reduced. However, there are still some drawbacks for the bare metal model, while it is more flexible and reliable for various applications. One of main drawbacks lies in that the bare metal virtualization architecture requires the support of hardware. Nonetheless, no all the physical servers provide such supports. In addition, the configuration of this model is also more complex than the hosted model. The hypervisor is available at the boot time of machine in order to control the sharing of system resources across multiple VMs. Some of these VMs are privileged partitions which manage the virtualization platform and hosted Virtual Machines. In this architecture, the privileged partitions view and control the Virtual Machines [11].

3 ADVANTAGES OF VIRTUALIZATION

There are several advantages to virtualization across several dimensions:

3.1 SECURITY

By compartmentalizing environments with different security requirements in different virtual machines one can select the guest operating system and tools that are more appropriate for each environment. For example, we may want to run the Apache web server on top of a Linux guest operating system and a backend MS SQL server on top of a guest Windows XP operating system, all in the same physical platform. A security attack on one virtual machine does not compromise the others because of their isolation.

3.2 RELIABILITY AND AVAILABILITY

A software failure in a virtual machine does not affect other virtual machines.

3.3 COST

It is possible to achieve cost reductions by consolidation smaller servers into more powerful servers. Cost reductions stem from hardware cost reductions (economies of scale seen in faster servers), operations cost reductions in terms of personnel, floor space, and software licenses. VMware cites overall cost reductions ranging from 29 to 64% [26].

3.4 ADAPTABILITY TO WORKLOAD VARIATIONS

Changes in workload intensity levels can be easily taken care of by shifting resources and priority allocations among virtual machines. Autonomic computing-based resource allocation techniques, such as the ones in [27], can be used to dynamically move processors from one virtual machine to another.

3.5 LOAD BALANCING

Since the software state of an entire virtual machine is completely encapsulated by the VMM, it is relatively easy to migrate virtual machines to other platforms in order to improve performance through better load balancing [28].

3.6 LEGACY APPLICATIONS

Even if an organization decides to migrate to a different operating system, it is possible to continue to run legacy applications on the old OS running as a guest OS within a VM. This reduces the migration cost.

4 VMWARE WORKSTATION

Virtualization is a proven software technology that is rapidly transforming the IT landscape and fundamentally changing the way people compute. Today, with powerful processing capabilities of X86 computer hardware just to run a single operating system and a single application, which makes most computer hardware resources are not fully utilized. Use of virtualization technology, a single physical machine can run multiple virtual machines, which can be shared between multiple environmental resources of the computer. Virtual machine is a tightly isolated software container; VMware Workstation virtualization software maps the physical hardware resources to virtual machine resources. So each virtual machine has its own CPU, memory, disk and network interface cards. In addition to the virtual machine can connect to the physical network adapter, CD-ROM devices, hard drives and USB devices, VMware Workstation can emulate other hardware. For example, the ISO file and it can be. Vmdk files, respectively, as CD-ROM and hard disk loading, we can also host to a virtual network adapter configured to use Network Address Translation (NAT), rather than for each virtual machine is allocated an IP addresses. Therefore, the virtual machine with the physical hardware does not have a lot of unique advantages:

4.1 COMPATIBILITY

The same physical machine, virtual machine carries its own guest operating systems and applications, and has all the components on the physical computer. Therefore, the virtual machine with all standards x86 operating systems, applications and device drivers are fully compatible, so that you can use virtual machines to run on physical x86 computers running all the same software.

4.2 ISOLATION

While virtual machines can share a computer's physical resources, but they remain completely isolated from each other, just as they are different physical computer. For example, if a single physical server with four virtual machines, and one of the virtual machine crashes, the other three virtual machines are still available. The availability and security, virtual environment applications running much better than in the traditional reason for non-virtualized applications running on the system, isolation is an important reason.

4.3 ENCAPSULATION

Virtual machine is essentially a software container, it will set of virtual hardware resources and operating system and all applications bundled or packaged in a package. Package to a virtual machine with exceptional mobility and ease of management. For example, you can move virtual machines from one location to another location and copy move and copy just the same as any other software.

4.4 INDEPENDENT OF THE HARDWARE

Virtual machine is completely independent of their underlying physical hardware. For example, you can configure the virtual machine exists on the underlying hardware and physical components of a completely different virtual components. The same physical server, each virtual machine can even run different types of operating systems [9].

5 ENCRYPTED DATA STORAGE

Since data in the cloud will be placed anywhere, it is important that the data is encrypted. We are using secure co-processor as part of the cloud infrastructure to enable efficient encrypted storage of sensitive data. One could ask us the

question: why not implement your software on hardware provided by current cloud computing systems such as Open Cirrus? We have explored this option. First, Open Cirrus provides limited access based on their economic model (e.g., Virtual cash). Furthermore, Open Cirrus does not provide the hardware support we need (e.g., secure co-processors). By embedding a secure co-processor (SCP) into the cloud infrastructure, the system can handle encrypted data efficiently (see Figure 5). Basically, SCP is a tamper-resistant hard-ware capable of limited general-purpose computation. For example, IBM 4758 Crypto-graphic Coprocessor (IBM) is a single-board computer consisting of a CPU, memory and special-purpose cryptographic hardware contained in a tamper-resistant shell, certified to level 4 under FIPS PUB 140-1. When installed on the server, it is capable of performing local computations that are completely hidden from the server. If tampering is detected, then the secure coprocessor clears the internal memory. Since the secure coprocessor is tamper-resistant, one could be tempted to run the entire sensitive data storage server on the secure co-processor. Pushing the entire data storage functionality into a secure co-processor is not feasible due to many reasons. First of all, due to the tamper-resistant shell, secure co-processors have usually limited memory (only a few megabytes of RAM and a few kilobytes of non-volatile memory) and computational power (Smith, 1999).Performance will improve over time, but problems such as heat dissipation/power use (which must be controlled to avoid disclosing processing) will force a gap between general purposes and secure computing. Another issue is that the software running on the SCP must be totally trusted and verified. This security requirement implies that the software running on the SCP should be kept as simple as possible. So how does this hardware help in storing large sensitive data sets? We can encrypt the sensitive data sets using random private keys and to alleviate the risk of key disclosure, we can use tamper-resistant hardware to store some of the Encryption/decryption keys (i.e., a master key that encrypts all other keys). Since the keys will not reside in memory unencrypted at any time, an attacker cannot learn the keys by taking the snapshot of the system. Also, any attempt by the attacker to take control of (or tamper with) the co-processor, either through software or physically, will clear the co-processor, thus eliminating a way to decrypt any sensitive information. This framework will facilitate (a) secure data storage and (b) assured information sharing. For example, SCP scan be used for privacy preserving information integration which is important for assured information sharing [10].

6 RELATED WORKS

Many studies were dedicated to provide a secure virtualized environment in cloud computing. Here are some of them: In [12], 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. VMware ESX server (hypervisor) runs on the bare hardware and provides ability to create VMs and move them from one PM to another using VMotion [13]. It requires the PM to have shared storage such as SAN or NAS. The cited paper [14] provides an overview of the memory management scheme employed in the ESX server. VMWare has the Virtual Center which provides a management interface to the virtual farm. Although some metrics are provided by the Virtual Center, they are not fine-grained and require extensive human interaction for use in management. Resource management of these virtual machines still needs to be addressed in a cost effective manner whether in a virtual server farm or in a grid computing environment as pointed out in [15]. A complete outline on various researches and trends in cloud computing has been presented in [16].The authors discuss a scheme for secure third party publications of documents in a cloud. Next, the paper will converse secure federated query processing with map Reduce and Hadoop, and discuss the use of secure co-processors for cloud computing. Finally, the authors discuss XACML implementation for Hadoop and discuss their beliefs that building trusted applications from untrusted components will be a major aspect of secure cloud computing [17]. A good report has been presented in [18]. Another good report on various architectural strategies is used by cloud computing in oracle white paper [19].

7 PROPOSED WORK

In the wake of intensive use of server hardware and allied resources, the two factors which weigh in during operations are power and cooling. At any given point of time, for any server virtualization to be classified as being a success, the overriding consideration is efficacy. Unbridled consumption of power can be a cause of great concern for businesses seeking an all-round optimization and utilization of resources. In a private cloud computing environment, where data processing and storing take place on a 24x7 basis, it is hardly a wonder that cooling would be of paramount concern, in addition to regulation of power consumption. Studies have shown that operating temperatures can soar significantly inasmuch within a virtualized environment as without. Therefore, it becomes inevitable that hardware resources be closely monitored and run in an environment which does not allow a server virtualization system to run at “hot” temperatures for any length of time. In

our proposed work first we want to show a detailed cost comparison that based on power and cooling has been drawn in a table format between physical server and VMware server [VMware esx] in fig2.In this table all figures and estimations are near approximations. Actual figures may vary. Servers require a high amount of cooling. It has been estimated that cooling costs alone amount to almost a good proportion of the actual power consumed during operation. It has been estimated, based on detailed calculations as presented in the, that server virtualization would help save a lot of money over a three-year period. Secondly we define hypervisor-secure virtualization as protection of a VM's data, and provide a concrete architectural solution which describe in fig3. The focus of the protections is on the storage, as this is where data resides, during a VM's execution.VM Data would be channeled through the secure co-processor for encryption. The Billboard Manager would then position the encrypted data in locations which it calculates to be optimum considering the parameters within which it has been designed to operate. Cryptographic co-processors help in defining the security protocols and implement them. A dedicated set of hardware forms a Cryptographic co-processor which can only take care of either encryption or decryption [20]. Billboard Manager helps to choose the appropriate storage location to store the encrypted data. A major part of our system is Billboard Manager which is to handle a large number of storage nodes. Billboard Manager knows the available blank space of cloud storage. Necessary collected encrypted data sends different suitable cloud storage.

BILLBOARD MANAGER FOLLOWS THIS ALGORITHM.

1) BM stores all information about Cloud storage Nodes like capacity, IP address, and shortest node distance and any kinds of information about the nodes.

2) All Cloud nodes send periodic information to BM.
   a) Channel capacity
   b) Storage space

Both of the information varies time to time and also area to area.

3) Now for t=0, compare storage capacity if the storage capacity >0

   Continue;
   Else stop

4) Compare storage capacity, choose the maximum one.

5) If the storage capacity of the two Cloud nodes to handover is same,

6) Compare the data rate. Choose the highest data rate.

   Else go back to 4

7) Repeat 4-6 every time while choosing a new cloud storage node to handover.

8) Make a list of the available cloud storage node and store it to BM

9) Now BM again makes a list of available cloud storage node based on free space.

10) Now comparing the best cloud storage node to send the data.

11) Now the connection is established.

Here we have launched 10 numbers of physical servers into two numbers of VMware ESX servers, for this cost of power and cooling became decreased. we have also shown a detailed cost comparison that based on power and cooling has been drawn in a table format between previous status (10 numbers of physical server) and present status (2 numbers of VMware server esx servers) in table1. In this table all figures and estimations are near approximations. Actual figures may vary. Thus we see the actual benefit for this migration, a lot of money is saving for this technology.

Table1 - Cost comparison table [21, 22, 23, 24]

COST OF POWER: PHYSICAL SERVER VS VMWARE V SPHERE DEPLOYMENT		
Charge description: physical Server	**Qty/Amt**	**Unit**
Power Rating/ Physical Server	0.5	Kw / Hr
Hours / Day	24	Hours
Days / Year	365	Days
Years Considered maintenance cycle for one server	3	Year
Total power Consumed per server	13140	Kw / Hr / Server
Approx. unit rate of commercial electrical Supply	9.00	Rs./ kW/ hr
Total cost of power per server	118260.00	Rs./ Server
Charge description: Virtual Server [VMware ESX]	**Qty/Amt**	**Unit**
Power Rating /Physical Server for Virtualization	1.5	kW/hr
Hours/Day	24	Hours
Days/ Year	365	Days
Years Considered Par Maintenance cycle for one server	3	Years
Total power consumed per server	39420	kW/hr/server
Approx. unit rate of commercial electric supply	9.00	Rs./kW/hr
Total cost of power per server	354780.00	Rs./Server
Number of physical server required in our scenario	2	Server
Therefore, total power cost to be met over 3 year	709560.00	Rs.
Savings expressed in terms of power cost over 3 years	**473040.00**	**Rs.**

COST OF COOLING: Physical Server vs. VMware vSphere deployment		
Charge description: Physical server	**Qty/Amt.**	**Unit**
Total cost of power required for cooling per server (approx.)	118260.00	Rs./Server
Number of physical servers required in our scenario	10	Server
Approximate effective rate of power required per server	0.75	
Therefore, total power cost for cooling to be met over 3 year	886950.00	Rs.
Charges description: Virtual Server [VMware ESX]	**Qty.**	**Unit**
Number of physical server required in our scenario for Virtualization	2	Server
Approximate effective rate of power required per server	0.75	Factor
Therefore, total power cost for cooling to be met over 3 years	177390.00	Rs.
Savings expressed in terms of power cost for cooling over 3 years	**709560.00**	**Rs.**

Savings Expressed in tems of power cost over 3 years	**473040.00**
Savings Expressed in tems of power cost for cooling over 3 years	709560.00
Total savings spread over 3 years with VMware vSphere Virtualization	**1182600.00**

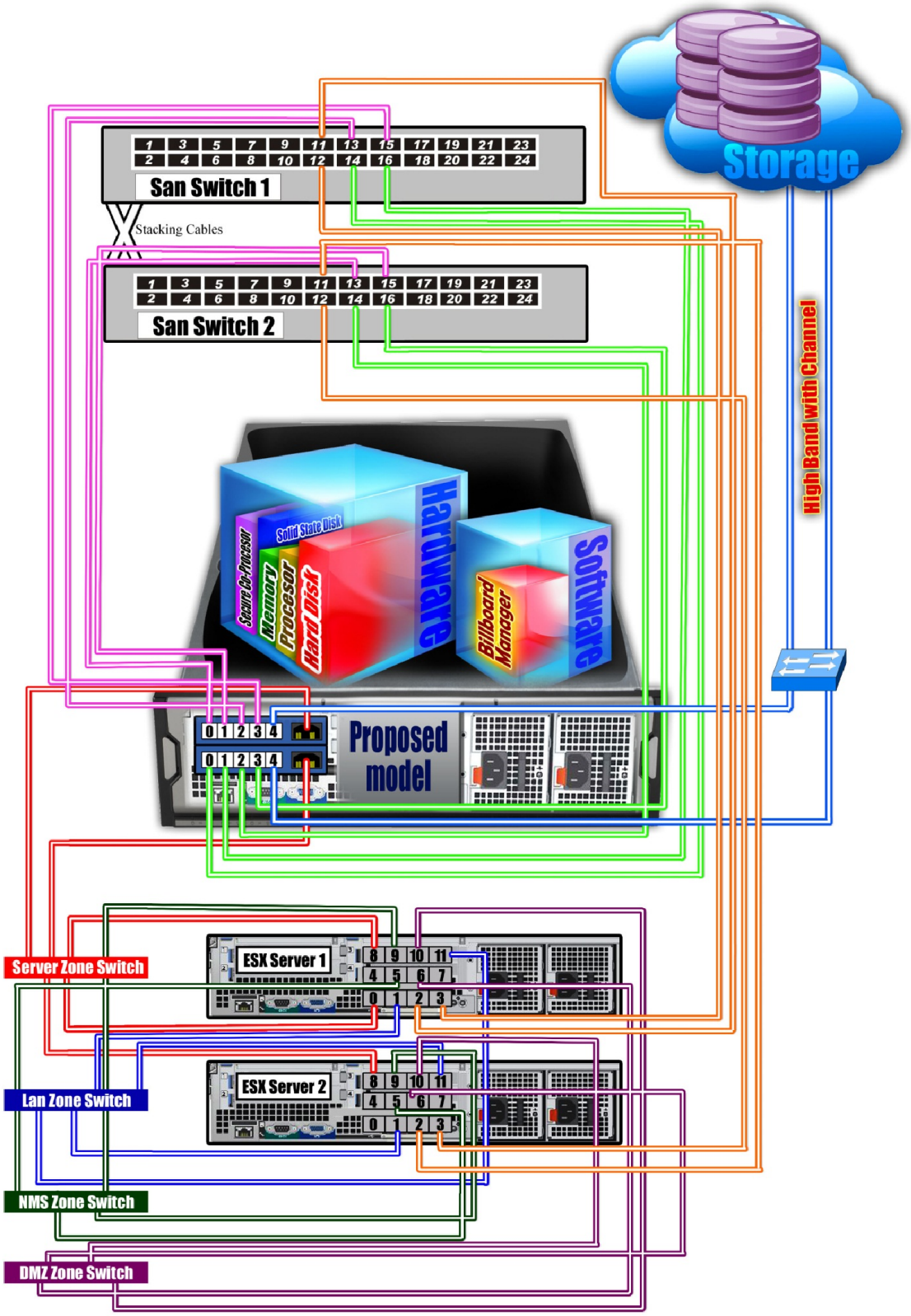


Fig.2. A Secure Cloud Datacenter Architecture

8 CONCLUSION

With rapid strides taken by businesses in order to survive and, indeed, thrive, so has the demand to deploy IT assets to support such has spiraled upwards. However, the pace of acquisition of IT assets – both hardware as well as software – have seen an emergence, of what is known in industry parlance, as "server sprawl". This is a phenomenon which sees low server utilization coupled with high system procurement and management costs – an unwanted and potentially crippling effect for businesses which operate on a basis of just-in-time principle. Studies conducted have revealed that the negative effects of "server sprawl" can be mitigated by a system of "server virtualization". The backing up process of VM files itself can compound recurring costs at an unexpected rate in the form of frequent acquisition of storage hardware in which to store the VM files. In this paper, we analyze the role that the Billboard Manager has to play in shuttling the VM files in a secure and encrypted manner so as to extract the maximum operating potential of server virtualization and virtualization storage system in a private cloud domain. Introduction of the Billboard Manager can play a pivotal role by optimizing the load demands placed on the individual physical server hardware as well as operations concerning the virtual machines hosted on them. Optimization of read/write cycles to be determined by the Billboard Manager would lead not only to a cooler operating cycle of the hardware, but would also result in a more "best-used" approach for the individual hardware resource itself.

REFERENCES

[1] Vijayaraghavan Soundararajan and Kinshuk Govil, "Challenges in building scalable virtualized datacenter management," SIGOPS Oper. Syst. Rev., vol. 44, no. 4, pp. 95–102, Dec. 2010.

[2] Luiz André Barroso and Urs Hölzle, "The case for energy-proportional computing," Computer, vol. 40, no.12, pp. 33–37, Dec. 2007.

[3] V. Chaudhary, M. Cha, J. Walters, S. Guercio, and S. Gallo, "A comparison of virtualization technologies for hpc," in Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on, March 2008, pp. 861 –868.

[4] S. A. Herrod, "Systems research and development at VMware," SIGOPS Oper. Syst. Rev., vol. 44, pp. 1–2, December 2010.

[5] Timothy Wood, Ludmila Cherkasova, Kivanc Ozonat, and Prashant Shenoy, "Profiling and modeling resource usage of virtualized applications," in Proceedings of the 9th ACM/IFIP/USENIX International Conference on Middleware, New York, NY, USA, 2008, Middleware '08, pp. 366–387, Springer-Verlag New York, Inc.

[6] Ludmila Cherkasova, Diwaker Gupta, and Amin Vahdat, "Comparison of the three cpu schedulers in xen," SIGMETRICS Perform. Eval. Rev., vol. 35, no. 2, pp. 42–51, Sept. 2007.

[7] Diego Ongaro, Alan L. Cox, and Scott Rixner, "Scheduling i/o in virtual machine monitors," in Proceedings of the fourth ACM SIGPLAN/SIGOPS international conference on Virtual execution environments, New York, NY, USA, 2008, VEE '08, pp. 1–10, ACM.

[8] Google Compute Engine, "http://cloud.google.com/compute," 2012.

[9] Xuyi Wei, Based on VMware technology's Campus network cloud platform technology research, 2012 IEEE International Conference on Computer Science and Electronics Engineering.

[10] C.Kishor Kumar Reddy, P.R Anisha, K. Srinivasulu Reddy, S. Surender Reddy, Third Party Data Protection Applied To Cloud and Xacml Implementation in the Hadoop Environment With Sparql, *IOSR Journal of Computer Engineering (IOSRJCE)* ISSN: 2278-0661 Volume 2, Issue 1 (July-Aug. 2012), PP 39-46.

[11] Farzad Sabahi, Secure Virtualization for Cloud Environment Using Hypervisor-based Technology, *International Journal of Machine Learning and Computing*, Vol. 2, No. 1, February 2012.

[12] Lombardi, F., Di Pietro, R.: Secure virtualization for cloud computing. *Journal of Network and Computer Applications*, 34(4), (2011).

[13] http://www.vmware.com/

[14] C.A. Waldspurger, "Memory resource management in VMware ESX server," Proceedings of the Fifth Symposium on Operating Systems Design and Implementation (OSDI'02), 2002.

[15] R. J. Figueredo, P. A. Dinda, and J. A. B. Fortes, "A case for Grid Computing on Virtual Machines" Proceedings of the 23rd International Conference on Distributed Computing Systems, 2003.

[16] Mr. D. Kishore Kumar, Dr. G. Venkatewara Rao, Dr. G. Srinivasa Rao, Cloud Computing: An Analysis of Its Challenges & Security Issues, *International Journal of Computer Science and Network (IJCSN)* Volume 1, Issue 5, October 2012.

[17] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, Security Issues for Cloud Computing, *International Journal of Information Security and Privacy*, 4(2), 39-51, April-June 2010.

[18] Robert Gellman, —WPF REPORT: Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, February 23, 2009.
[19] Oracle White Paper in Enterprise Architecture – Architectural Strategies for Cloud Computing.
[20] Praveen Ram C, Sreenivaasan G, Security as a Service (SasS), Securing User Data by Coprocessor and Distributing the Data,978-1-4244-9008-0/10/$26.00 ©2010 IEEE
[21] Why Virtualize: Server Consolidation, Business Continuity http://www.vmware.com/virtualization/why-virtualize.html
[22] Why Choose VMware Virtualization for your Virtual Infrastructure http://www.vmware.com/technical-resources/advantages/
[23] No Compromise, Cost Effective VMware Storage for the SMB http://virtualizationreview.com/white papers/2012/02/drobo-no-compromise-cost-effective-vmware-storage-for-the-smb.aspx?tc=page0
[24] Gartner: PCs Out, 'Personal Cloud' In by 2014 – Virtualization Review http://virtualizationreview.com/articles/2012/03/22/personal-cloud-by-2014.aspx
[25] Farzad Sabahi, Secure Virtualization for Cloud Environment Using Hypervisor-based Technology, *International Journal of Machine Learning and Computing,* Vol. 2, No. 1, February 2012.
[26] VMware, "Consolidating Mission Critical Servers," www.vmware.com/solutions/consolidation/mission critical.Html
[27] M.N. Bennani and D.A. Menasc´e, "Resource Allocation for Autonomic Data Centers Using Analytic Performance Models," Proc. 2005 IEEE International Conference on Autonomic Computing, Seattle, WA, June 13-16, 2005
[28] R. Uhlig et. al., "Intel Virtualization Technology," IEEE Internet Computing, May 2005, Vol. 38, No. 5

AUTHORS

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.

Rajesh Bose is a senior project engineer employed by Simplex Infrastructures Limited at the company's Data Center located in Kolkata. He completed his M.Tech. in Mobile Communication and Networking from WBUT in 2007. He had also completed his B.E. in Computer Science and Engineering from BPUT in 2004. His research interests include cloud computing, wireless communication and networking.