Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Green Cloud Computing: A Virtualized Security Framework for Green Cloud Computing

Mr. Anup R. Nimje [1]
M.E. Research Student,
Computer Engineering
Sipna COET, Amravati, India.

Prof. V. T. Gaikwad[2]
Asso.Professor,HOD
Information Technology
Sipna COET, Amravati, India.

Prof. H. N. Datir[3]
Asst.Professor,
Computer Sci & Engg.
Sipna COET, Amravati, India.

Abstract—In the IT industry's there is forcefully demand of the technology known as Cloud computing. It is an emerging trend in computing. There are huge data centres are used in big industries. Environmentally, these systems can produce e-wastes, harmful gases with heat. This paper focuses on security in such a power saving data centres in the enterprises we called them as Green Cloud Computers. We have explained and suggested the Virtualization technique for saving energy and the security framework for the Green Cloud that consist of pool of virtual machines. This security framework consists of policy enforcement, trust management and such a security model.

Keywords— Cloud computing, Green cloud computing, Virtualization, security, policy, energy efficiency.

I. INTRODUCTION

"Green computing" is the use of computing with environment responsibility. These practices include the energy efficient peripheral of the computing system and the energy efficient processors (CPU's), servers at various data centres or cloud centres. It also consists of reduced resources use and proper "e-waste" management.

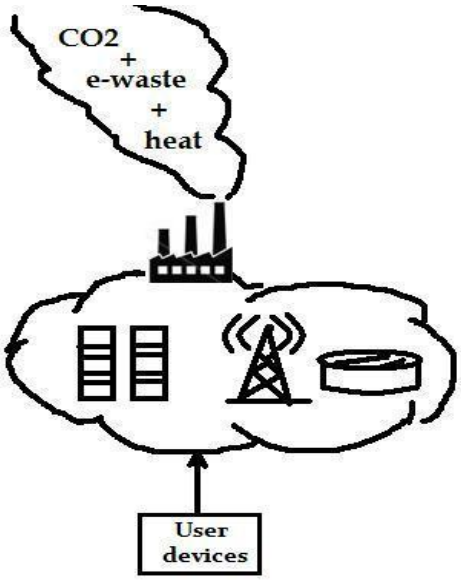

Fig.-1 A non-green system

Similarly, the term *"green cloud computing"* gives environmentally beneficial, with cloud computing, programs, services run on our infrastructure or platform or we can say on our system, so there is no requirement for separate system for traffic management. Cloud computing allows us to run at high utilization of resources; you can use fewer number of computers this allows us to have higher utilization, saving on environment cost of building those computers.[1] Centralization of an IT infrastructure to from cloud computing also creates flexibility. It is clear that with energy demand in computing is increasing and it gets shifted to cloud computing that is to become green. In this paper we are going to explore how the virtualisation technique can help to make the cloud system green and the security framework for cloud VM pool and how the virtualization is the better solution for it. Due to increasing demand and development with the energy efficient [2] and environment eco-friendly infrastructure is needed. In general, cloud computing is still having the security concerns for adopting cloud computing, hence green computing. In IT infrastructure and industries, privacy and integrity is needed. The successful implementation of cloud computing is when it is adopted over a large scale users. There should be resource management and network between users. In virtual machines (VM) of different users reside on

the same machine and share the same LAN. Hence security risks are high. Hence in cloud computing, it may be shared with hackers in the cloud. Virtualization based cloud computing platforms are becoming very popular that provides a new supplement, consumption and delivery model for network software application over the internet. Virtualization refers to the abstraction of computer resources or the processes of two or more operating system on a single hardware machine. A cloud is a pool of virtualized computer resources. Virtualization consists of a system admin to combine physical systems into VM in maximally energy efficient manner. That is necessarily in green cloud computing point of view to less power consumption. Virtualization assists in workload distribution and management. Based on software cloud model, a virtualized, scalable and energy efficient resource management strategy can be developed to provide interaction to loosely coupled resources. It gives significantly improved utilization.

II. GREEN COMPUTING AND NEED OF VIRTUALIZATION

Cloud computing cannot be always suitable for ecology [5]. The recent studies confirmed that rely on a server is generally more environmentally friendly, although care must be taken to a whole series of parameters to calculate the best real efficiency of the clouds. According to a new research from Pike Research [3], the global market for green data centers will grow from $17.1 billion in 2012 to $45.4 billion by 2016. In other words, the data centers impact on real environment by producing heat. It is also important to keep in mind that a data center has a more environmental impact than a system. The research was based on setups those include virtualization and without virtualization. It is found that on-site server with no virtualization will emit about 46kg of CO2 per year. The figure will touch 2kg if a person using a public cloud conforming to best practices. [4]

If data is stored on the public cloud whose servers are not that efficient, those servers are not well used and use electricity from higher-carbon-emitting sources. Thus, there could be some practices by which servers can be run with greener solutions. Also, studies also proved that cloud systems are more energy efficient and carbon efficient than that of an ordinary system.

About cloud computing (fig.-1), it consists of a concept of use of virtualization. And thus, virtualization is critical to cloud computing. It simplifies the delivery of services by providing a platform for optimizing complex IT resources in a scalable manner. That makes cloud computing so *cost effective*.

In cloud computing it needs to support many different operating environments, to manage the various aspects of virtualization in cloud computing most companies use *hypervisors.* The hypervisors can support different operating system environment hence, the hypervisor becomes an ideal delivery mechanism by allowing you to show the same application on lots of different systems. Because hypervisors can load multiple operating systems, they are a very practical way of getting things virtualized quickly and efficiently.

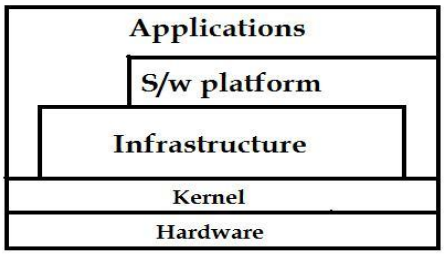

Fig.-2 Cloud computing: basic model

Hypervisor-Based Virtualization can be explained as follows:-

Virtualization makes easing the administrative burden of deploying, managing, delivering resources, and providing the ability for end users to request and use virtualized resources. Virtualized hypervisor environment and can utilize additional security tools such as intrusion detection systems.[6] However, it is vulnerable because the hypervisor has a single point at which it comes across failure. In case, if the hypervisor gets crashed or the attacker gains control over it or hacks it, then all VMs are under the attacker's control. However, taking control over the hypervisor from the virtual machine level user is difficult, though not impossible.

The VM pool consists of the number of OS environment and as system boots, the hypervisor is available for controlling of system. It is analogous to VMM. Some of these VMs are given privileges and those can manage the virtualization platform and hosted Virtual Machines (VM). In this architecture, the privileged partitions view and control the Virtual Machines. This approach establishes the most controllable and secured virtualization and also it can prevent various misbalancing and security concerns for the VM pool. The hypervisor is a software component which controls access to the physical hardware. (Fig.2) It may run on top of a host operating system, allowing other operating systems to run within this host OS, and so on the same physical hardware. The latter inherently gives lower performance, since it has to go through more layers of software to access the physical resources.

Cloud Computing may look like Virtualization because it appears that your application is running on a virtual server detached from any reliance or connection to a single physical host. However, Cloud Computing can be better described

as a service where Virtualization is part of a physical infrastructure. Cloud Computing builds on top of a virtualized infrastructure using standardization and automated delivery to provide service management. Thus, it makes monitoring of the virtualized resources and the deployment of these resources possible. Virtualization is a necessary for adopting a cloud computing infrastructure. [7]

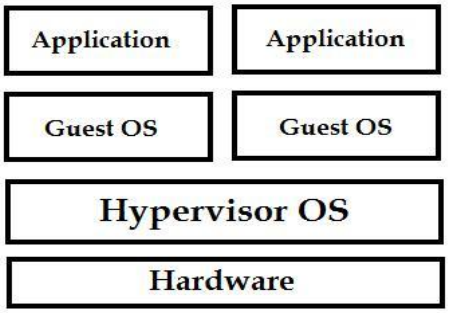

Fig.- 3 Virtualization with hypervisor OS

III. FEW SECURITY CONCERNS IN VM IMPLEMENTATION

There are some security concerns around the use of virtualization, even before you consider using it for cloud computing. These can be explained as follows.

1. First, addition of a new VM, is the addition of an Operating System. It is a security risk for your clouds system Every OS should be appropriately patched, maintained and monitored.
2. Second, typical network-based intrusion detection cannot work well with virtual servers on the same host. Hence there must be authentication provider or there must be a secured access.
3. Consequently, an advanced technique to monitor traffic between VMs is needed. When the data is moved between multiple physical servers, however, load balancing or failover, network monitoring systems can't assess and cannot perform their operations. So, there must be scheduling and monitoring.

IV. SECURITY FRAMEWORK

In this section, we explore a security framework that is to be designed for cloud system which consists of VM-pool(s). It is based on virtualized security solution developed for green cloud computing by *Jianxin Li et al* [8]. That can give authentication, access control and trust through portals. We here only focus on the trust management that is, security framework for the green cloud computing. Authentication, digital certification and also the Policy decision and we can say that policy enforcement is also provided. Trust management mechanism is also given. Policy based access control for sharing a resource sharing that across multiple resources pools. For synchronisation or co-ordination or monitoring the system we provided scheduler.

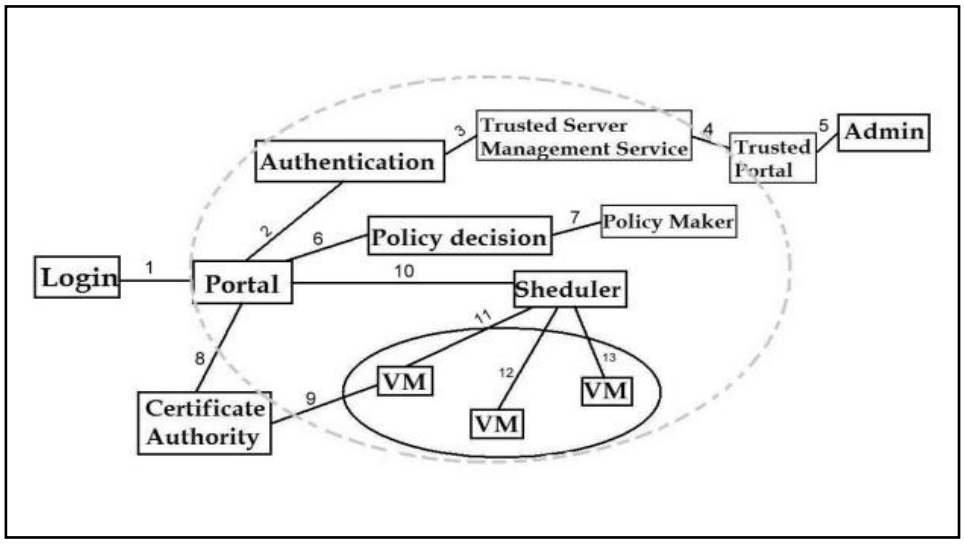

Fig.- 4 Framework for security in a VM pool

We can have the Policy-based security for the local VM pool. In a VM pool, many physical machines are connected in a high-speed network, and every physical machine can run several virtual machines simultaneously. In this pool, users can create their own virtual clusters by connecting assigned virtual machines. The security policy for this

virtual machine pool is configured in a centralized portal, and it *authenticates the user and manages the access control policies of virtual machines.*

As shown in Fig. 4 we can have the various steps in the security mechanism in a VM pool. These can be explained as follows:

At first, a user logs-in the virtual machine pool with their password or certificate, there is a portal provided which performs next steps. There is authentication mechanism which consists of authentication server and trusted server management service. The authentication server in the VM pool verifies the identity of the login user and also manages trust; then the user is able to create virtual cluster on the portal workspace for performing its operation or gets the requested service. Before performing the tasks by user, it must be verified and trusted in order to ensure the security, there is a policy server provided for policy enforcement to the user. If all the actions involved in this task are permitted by the policy decision mechanism, then this task is submitted to the scheduler. After task information is submitted to the scheduler, the portal submits a description file of the user's task to the scheduler. Then, the scheduler deploys the virtual machines according to the description of the task file and pool information service. After a virtual cluster or a virtual lab is deployed in the VM pool, then the user can access directly related virtual machines in this pool via remote client tools. The operations are performed by the certificate authorization. The user can access the virtual machine through SSH (Secure Shell) or VNC (Virtual Network Computing) protocols. At the policy server, whatever the policies required are stored at policy maker server. The policy stored consists of user level, VM or VM-pool attributes, and constraints of operations to be performed.

In case of multiple pools:-

Now consider a system that consists of two or more VM pools. So, as given by *Jianxin Li et al* [8]; for cloud computing there should be trust management system that should be maintained by the security party of cloud service provider for their users. There is admin and trust portal that is provided for trust management and that can be explained as given below:

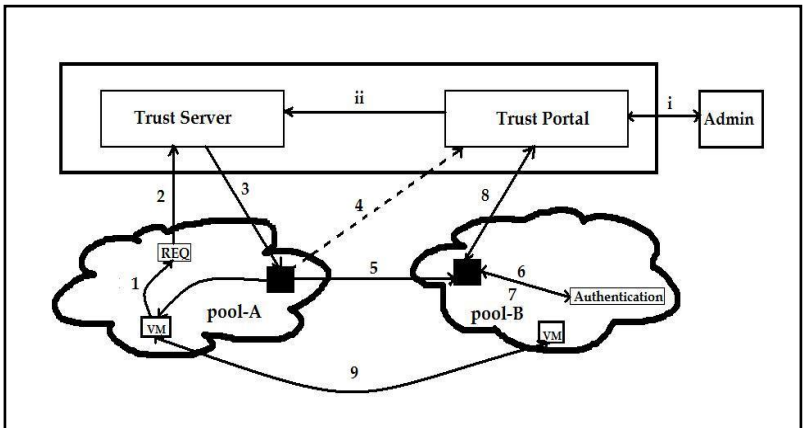

Fig.-5 Security Management for accessing multiple pools of VM's

There can be a trust management for accessing multiple pools.[8] The various steps involving in this mechanism according to the above fig.-5, various steps are as follows:

Admin controls trust management server with the trust portal. When a VM user from pool-A wants to access or to be connected with a VM in pool-B, it sends request REQ to the trust server (1,2). The trust server checks for authentication and sends response (3). And again authentication is checked at pool-B authentication server (5,6,7). Also it is monitored by trust portal (8). When it is granted, VM can get access with another VM in pool-B (9). User can access the remote VM in another pool by virtual network secured protocol.

V. DISCUSSION ON ENERGY SAVING AND RELATED WORK

How it works as in the green cloud computing:

Let's discuss about how virtualization makes cloud green or eco-friendly. We know, the data center consumes the power as huge as that can be used to power thousands of homes. The environmentalists and computer scientists are working on reducing the huge amount of power used and make data centers more energy-efficient than they currently are.

The virtualization can be the solution for it. It can be used to reduce power consumption by data centers. The main purpose of the virtualization is that to make the most efficient use of available system resources, including energy. A data center, installing virtual infrastructure allows several operating systems and applications to run on a lesser number of servers, it can help to reduce the overall energy used for the data center and the energy consumed for its cooling. Once the number of servers is reduced, it also means that data center can reduce the building size as well. Some of the advantages of Virtualization which directly impacts efficiency and contributes to the environment include: Workload balancing across servers, Resource allocation and sharing are better monitored and managed and the Server utilization rates can be increased up to *80%* as compared to initial *10-15%*. The energy saved per server would be near about *7000 KWH* per year.[9] It means that there would be large saving of energy, hence virtualization is the best practice for Green Cloud Computing especially in the developing countries like India. Where the power saving is the today's need**.**

VI. CONCLUSION

We have discussed about the cloud computing in the environmental point of view and we explored the concept of Green Cloud Computing. Then we explored the general deployment model of Cloud computing and the Concept of Virtualization. Then we explored the security framework for the pool of Virtual Machines (VM), the authentication and the trust management and policy enforcement into the system. Then we explored the trust management or authentication mechanism for multiple pool system. Then we said that the virtualization technique is the best solution for making the green cloud computing and the use of virtualization can be the most beneficial which includes load balancing, resource management , server utilization and the most importantly, power savings. That makes the ordinary data centre Cloud Computing, the *'Green'* Cloud Computing.

REFERENCES

[1] Jan Kremer , "Cloud Computing Virtualization" (White paper on virtualization)
[2] Qilin Li, Mingtian Zhou "The Survey and Future Evolution of Green Computing" IEEE/ACM International Conference on Green Computing and Communications,
[3] Pike Research Article on green date center (http://cloudtimes.org/2012/10/01/green-data-center-market-pike-research/)
[4] How green is cloud computing, new study (http://cloudtimes.org/2012/10/28/how-green-is-cloud-computing-new-study/)
[5] Cloud Environment Sustainability (http://www.cloudbus.org/papers/Cloud-EnvSustainability)
[6] Secure Virtualization for Cloud Environment Using Hypervisor-based Technology, Farzad Sabahi, *Member, IEEE*
[7] Irfan Rizvi, "Hardware Virtualization Models"
[8] Jianxin Li et al "CyberGuarder :A virtualization security assurance architecture for green cloud computing" Future Generation Computer Systems
[9] Article: Netmagicsolutions.com

