# Importance of Cloud Computing and its Security Issues in Network Virtualization Process

Sumit Kumar, Sumeer Kumar

**Abstract: In this manuscript, the cloud computing and its security issues have been demonstrated in case of Network virtualization process. Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet). Cloud computing is one of today's most exciting technologies, because it can reduce the cost and complexity of applications, and it is flexible and scalable. These benefits changed cloud computing from a dreamy idea into one of the fastest growing technologies today. Actually, virtualization technology is built on virtualization technology which is an old technology and has had security issues that must be addressed before cloud technology is affected by them. In addition, the virtualization technology has limit security capabilities in order to secure wide area environment such as the cloud. Therefore, the development of a robust security system requires changes in traditional virtualization architecture. This paper proposes new security architecture in a hypervisor-based virtualization technology in order to secure the cloud environment.**

**Index Terms: Virtualization, cloud computing, architecture, security, hypervisor.**

## I. INTRODUCTION

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network.[1] At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rackspace, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

In the past decades, the world of computation has experienced some dramatic changes from stand alone application to client-server architecture and from distributed to service oriented architecture. All of these transformations aimed to make the software easier to use and improve business process execution efficiency [1]. Cloud computing, an emerging IT delivery model, is the next generation of networking computing which can deliver both software and hardware as on-demand resources and services over the internet with lower IT costs and complexities [2]. Many companies such as Amazon, IBM, Google, Oracle, Microsoft, Sales force and HP are rushing to provide cloud solutions in various ways. Cloud computing, the hottest buzzword in the IT area, has been frequently discussed in workshops, conferences and even magazines [5]. Nevertheless, to define cloud computing is not an easy task, confusion still remains about what exactly the definition of cloud computing is. From different perspectives, there are more than a dozen definitions for cloud computing in academia [7]. But the following features of cloud computing defined among them are common:

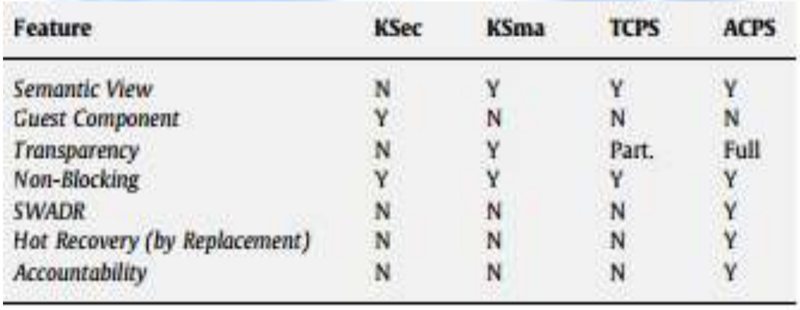
- Cloud computing is a computing platform to enable resource sharing in terms of scalable infrastructures, middleware and application development platforms and applications.
- New computer technologies, such as service oriented architecture, virtualization, high power enterprise servers and high band width, support to realize cloud computing platforms.
- Typically, services provided in clouds can be grouped into 3 categories: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

Cloud computing enables users to store and process all their data on the web via the Internet, with no doubts security is one of main significant concerns [9] [26]. A more fundamental reason preventing companies from moving to cloud computing is that the cloud computing platform is inherently less secure than the traditional network infrastructure [10] [25]. Security must be integrated into every aspect of cloud computing platforms to make users trust that their data is secure [27]. One of biggest challenges of security issues in the design of a cloud computing platform is that of virtual machine (VM) instance interconnectivity [11]. Because users who are granted super-user access to their provisioned VMs, without care, may have possibilities that a VM can monitor another VM or access the underlying network interfaces, which we call the break of isolation. In this paper, we focus on network security for virtual machines and we select the open source project - Xen hypervisor as the research platform. In this work, we discuss and analyze the network secure problems existed in VMs, and then present a novel virtual network model which can control the inter-communication among VM instances running on the hypervisor with higher secure.

## II. HISTORY & BACKGROUND

While privacy issues in clouds have been described in depth by Pearson (2009), cloud security is less discussed in the literature (Gu and Cheung, 2009). Some interesting security issues are discussed in Siebenlist (2009), while an almost complete survey of security in the context of cloud storage services is provided by Cachin et al. (2009). An exhaustive cloud security risk assessment has been recently presented by Enisa (2009). Also worth reading is the survey on cloud computing presented in Armbrust et al. (2009). These papers have been the starting points of our work and we refer to them in terms of problems and terms definition. Most current integrity monitoring and intrusion detection solutions can be successfully applied to cloud computing. File system Integrity Tools and Intrusion Detection Systems such as Tripwire (Kim and Spafford, 1994) and (AIDE) (AIDEteam, 2005) can also be deployed in virtual machines, but are exposed to attacks possibly coming from a malicious guest machine user. Furthermore, when an attacker detects that the target machine is in a virtual environment, it may attempt to break out of the virtual environment through vulnerabilities (very rare at the time of writing Secunia, 2009) in the Virtual Machine Monitor (VMM). Most present approaches leverage VMM isolation properties to secure VMs by leveraging various levels of virtual introspection. Virtual introspection (Jiang et al., 2007) is a process that allows to observe the state of a VM from the VMM. Sec Visor (Se sha dri et al., 2007) Lares (Payne et al., 2008) and KVM-L4 (Peter et al., 2009), to name a few, leverage virtualization to observe and monitor guest kernel code integrity from a privileged VM or from the VMM. Nickel (Riley et al., 2008) aims at detecting kernel root kits by monitoring the integrity of kernel code. However, Nickle does not protect against kernel data attacks (Rhee et al., 2009), whereas our solution does. Most proposals have limitations that prevent them from being used in distributed computing scenarios (e.g.. SecVisor only supports one guest per each host) or just do not consider the special requirements or peculiarities of distributed systems; for instance, KVM-L4 shares the same underlying technology as Lombardi and Di Pietro (2009) but the additional context switch ing overhead in the 64-bit scenario, representing the vast majority of cloud hosts, remains to be verified. Also worth citing are IBMon (Ranadive et al., 2009), a monitoring utility using introspection for asynchronous monitoring of virtualized network devices, and LoGrid (Salza et al., 2006), an example of autonomic reaction system.

**Table 1: Comparison of features provided by ACPS, TCPS, Kvm Sma (KSma) and Kvm Sec (KSec).**



| Feature | KSec | KSma | TCPS | ACPS |
|---|---|---|---|---|
| *Semantic View* | N | Y | Y | Y |
| *Guest Component* | Y | N | N | N |
| *Transparency* | N | Y | Part. | Full |
| *Non-Blocking* | Y | Y | Y | Y |
| *SWADR* | N | N | N | Y |
| *Hot Recovery (by Replacement)* | N | N | N | Y |
| *Accountability* | N | N | N | Y |

In an effort to make nodes resilient against long-lasting attacks, Self-Cleansing Intrusion Tolerance (SCIT) (Huang etal., 2006) treats all servers as potentially compromised (since undetected attacks are extremely dangerous over time).SCIT restores servers from secure image son regular basis. The drawback of sucha system is that it does not support long-lasting sessions required by most cloud applications. Similarly, VM-FIT (Distler etal.,2008) creates redundant server copies which can periodically be refreshed to increase the resilience of the server. Finally, Sousa etal.(2007) approach combines proactive recovery with services that allow correct replicas to react and be recovered when there is a sufficient probability that they have been compromised. Along with the many advantages brought by virtualization, there are additional technological challenges that virtualization presents, which include an increase in the complexity of digital forensics (Pollitt et al., 2008) investigations as well as questions regarding the forensics boundaries of a system.

Finally, the same authors of this paper proposed Transparent Cloud Protection System (TCPS)—appearing as a poster at SAC'10 (Lombardi and Di Pietro, 2010). That poster introduces some of the scenarios and requirements that are also common to ACPS, however they are only partly sketched in TCPS. In particular, ACPS and TCPS share the positioning of the monitoring system and the requirement that it has to be as much transparent as possible to guests. ACPS extends and completes the architecture just sketched in TCPS. For instance, ACPS enjoys unique features, such as the SWADR approach, the increased decoupling of action and reaction, the increased immunity and integrity of the platform as well as the integration with real-world architecture and the support for accountability. All these new relevant features, as well as extensive experiments on both security and performance, make the present proposal a novel Contribution.

## III. CLOUD RAS ISSUES

Using Cloud results applications and data will move under third-party control. The cloud services delivery model will create clouds of virtual perimeters as well as a security model with responsibilities shared between the customer and the cloud service provider. This shared responsibility model will bring new security management challenges to the organization's IT operations staff [4]. Predominantly, the first question is an information security officer must answer to that whether he has adequate transparency from cloud services to manage the governance (shared responsibilities) and implementation of security management processes such as detection and prevention solutions to assure the costumers that the data in the cloud is appropriately protected. Actually, the answer to this question has two parts: what security controls must the customer provide over and above the controls inherent in the cloud platform, and how must an enterprise's security management tools and processes adapt to manage security in the cloud. Both answers must be continually re-evaluated based on the sensitivity of the data and the service-level changes over time .

### A. Data Leakage

Innately, when moving to a cloud there is two changes for customer's data. First, the data will store away from the customer's local machine. Second, the data is moving from a single-tenant to a multi-tenant environment. These changes can raise an important concern that called data leakage. Because of them, Data leakage has become one of the greatest organizational risks from security standpoint . Nowadays, for mitigate effects of such problem there has been interested in the use of data leakage prevention (DLP) applications to protect sensitive data. But if data stored in a public cloud because of nature of it, using DLP products is valueless to protect the confidentiality of that data in all types of cloud. Inherently, in SaaS and PaaS discovery of client's data with DLP agents is impossible except when the provider put ability of it to its service. However, it is possible embedding DLP agents into virtual. Unlike the other types of clou, machine in IaaS to achieve some control over data associated. In private clouds, Costumer has direct control over the whole infrastructure; it is not a policy issue whether DLP agents are deployed in connection with SaaS, PaaS, or IaaS services. However, it may well be a technical issue whether DLP agents interoperate with your SaaS or PaaS services as architected . In hybrid cloud, if service is IaaS, client could set in DLP agents for some control over data.

### B. Cloud security issues

Innately, Internet is communication infrastructure for cloud providers that use well-known TCP/IP protocol which users' IP addresses to identify them in the Internet. Similar to physical computer in the Internet that have IP address, a virtual machine in the Internet has an IP address as well. A malicious user, whether internal or external, like a legal user can find this IP addresses as well. In this case, malicious user can find out which physical servers the victim is using then by implanting a malicious virtual machine at that location to launch an attack . Because all of users who use same virtual machine as infrastructure, if a hacker steals a virtual machine or take control over it, he will be able to access to all users' data within it. Therefore, The hacker can copy them into his local machine before cloud provider detect that virtual machine is in out of control then the hacker with analysis the data may be find valuable data afterward .

### Attacks in cloud

Nowadays, there are several attacks in the IT world. Basically, as the cloud can give service to legal users it can also service to users that have malicious purposes. A hacker can use a cloud to host a malicious application for achieve his object which may be a DDoS attacks against cloud itself or arranging another user in the cloud. For example, assume an attacker knew that his victim is using typical cloud provider, now attacker by using same cloud provider can sketch an attack against his victim. This situation is similar to this scenario that both attacker and victim are in same network but with this difference that they use virtual machines instead of physical network.

Most network countermeasures cannot protect against DDoS attacks as they cannot stop the deluge of traffic and typically cannot distinguish good traffic from bad traffic. Intrusion Prevention Systems (IPS) are effective if the attacks are identified and have pre-existing signatures but are ineffectual if there is legitimate content with bad intentions Unfortunately, similar to IPS solutions, firewalls are vulnerable and ineffective against DDoS attacks because attacker can easily bypass firewalls and also IPSs since they are designed to transmit legitimate traffic and attacks generate so much traffic from so many distinct hosts that a server, or for cloud its Internet connection, cannot handle the traffic. It may be more accurate to say that DDoS protection is part of the Network Virtualization layer rather than Server Virtualization. For example, cloud systems use virtual machines can be overcome by ARP spoofing at the network layer and it is really about how to layer security across multivendor networks, firewalls and load balances.

DDoS attacks are one of the powerful threats available in world, especially when launched from a botnet with huge numbers of zombie machines. When a DDoS attack is launched, it sends a heavy flood of packets to a Web server from multiple sources. In this situation, the cloud may be part of the solution. it's interesting to consider that websites experiencing DDoS attacks which have limitation in server resources, can take advantage of using cloud that provides more resource to tolerate such attacks. In the other hand, cloud technology offers the benefit of flexibility, with the ability to provide resources almost instantaneously as necessary to avoid site shutdown. Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements; usually any form of hardware that operates on a Blacklist pattern is quickly overrun and will become in out of-service situation. In cloud computing where infrastructure is shared by large number of clients, DDoS attacks make have the potential of having much greater impact than against single tenanted architectures.

## IV. Reliability and Security in Network Virtualization

Apart from security, there are reliability-related issues in virtualization that can affect performance of cloud. For example, the provider may combine too many Virtual Machines onto a physical server. This can result in performance problems caused by impact factors such as limited CPU cycles or I/O bottlenecks. These problems can occur in a traditional physical server, but they are more likely to occur in a virtualized server because of the connection of a single physical server to multiple Virtual Machines such that they all compete for critical resources. Thereby, management tasks such as performance management and capacity planning management are more critical in a virtualized environment than in a similar physical environment. This means that IT organizations must be able to continuously monitor the utilization of both physical servers and Virtual Machines in real time. This capability allows IT organizations to avoid both over- and underutilization of server resources such as CPU and memory and to allocate and reallocate resources based on changing business requirements.

This capability also enables IT organizations to implement policy-based remediation that helps the organization to ensure that service levels are being met [2]. Another challenge in Virtualization is that cloud organizations must now manage Virtual Machine sprawl. With Virtual Machine sprawl, the number of Virtual Machines running in a virtualized environment increases because of the creation of new Virtual Machines that are not necessary for business. Worries about Virtual Machine sprawl include the overuse of infrastructure. To prevent Virtual Machine sprawl, Virtual Machine managers should analyze the need for all new Virtual Machines carefully and ensure that unnecessary Virtual Machines migrate to other physical servers. In addition, an unnecessary virtual machine will able to move from one physical server to another with high availability and energy efficiency. However, consider that it can be challenging to ensure that the migrated Virtual Machine keeps the same security, QoS configurations, and needed privacy policies. It must be ensured that the

## V. Threats and Attacks in Network Virtualization

### A. Threats

In 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.

**Virtual machine level attacks:** Potential vulnerabilities are the hypervisor or Virtual machine technology used by cloud vendors are a potential problem in multi-tenant architecture . These technologies involve "virtual Machines" remote versions of traditional on-site computer systems, including the hardware and operating system. The number of these virtual Machines can be expanded or contracted on the fly to meet demand, creating tremendous efficiencies.

**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.

**Expanded network attack surface:** The cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases .

**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.

**Lock-in:** It seems to be a lot of angst about lock-in in cloud computing. The cloud provider can encrypt user data in particular format and if user decides to migrate to another vendor or something like .

**Data control in cloud:** For midsize businesses used to having complete visibility and control over their entire IT portfolio, moving even some components into the Cloud can create operational "blind spots", with little advance warning of degraded or interrupted service [10].

**Communication in virtualization level:** Virtual machines have to communicate and also share data with each other. If these communications didn't meet significant security parameters then they have potential of becoming attacks target.

### B. Attacks

Nowadays, there are several attacks in the IT world. Basically, as the cloud can give service to legal users it can also service to users that have malicious purposes. A hacker can use a cloud to host a malicious application for achieve his object which may be a DDoS attacks against cloud itself or arranging another user in the cloud. For example an attacker knew that his victim is using 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 same network but with this difference that they use virtual machines instead of physical network (Figure 1) [9].

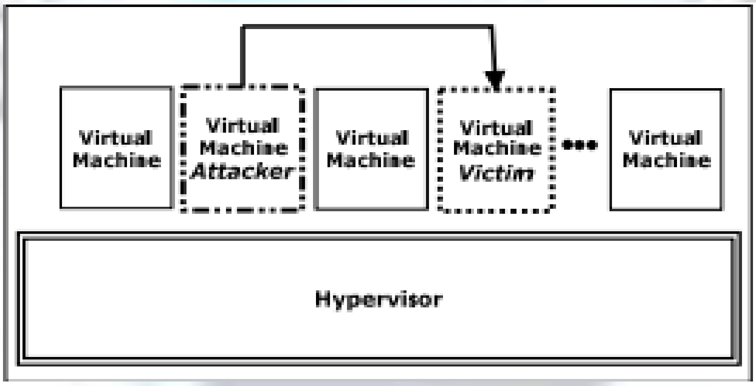


**Fig. 1: Attack scenario within cloud**

### 1) DDoS attacks

Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements; usually any form of hardware that operates on a Blacklist pattern is quickly overrun. In cloud computing where infrastructure is shared by large number of VM clients, DDoS attacks make have the potential of having much greater impact than against single tenanted architectures. If cloud has not sufficient resource to provide services to its VMs then maybe cause undesirable DDoS attacks. Solution for this event is a traditional solution that is increase number of such critical resources. But serious problem is when a malicious user deliberately done a DDoS attacks using bot-nets. It may be more accurate to say that DDoS protection is part of the Network Virtualization layer rather than Server Virtualization. For example, cloud systems use virtual machines can be overcome by ARP spoofing at the network layer and it is really about how to layer security across multivendor networks, firewalls and load balances.

### 2) Client to client attacks

One malicious virtual machine could infect all Virtual Machines that exist in physical server. An attack on one client VM can escape to other VM's that hosted in the same physical, this is the biggest security risk in a virtualized environment. When malicious user puts the focus on virtual machines become easy to access, the attacker has to spend time attacking one virtual machine, which can lead to infecting other VMs, and thereby escaping the hypervisor and accessing the environment level that officially it can't accessible from VM level. Hence, the major security risk in virtualization environments is "client to client attacks". In this attack an attacker gets the administrator privileges on the infrastructure level of virtualization environment and then can access to all VMs. If the hacker could also get control of the hypervisor and he owns all data transmitting between the hypervisor and VMs and he can perform attacks such as a spoofing attack.

## VI. Proposed Architecture

In this paper, the authors have added some features to virtualization architecture in order to improve security for cloud environment. When the workload of the VM increases abnormally, the VM may be a victim or an attacker" Therefore, in the architecture, the authors included additional units for monitoring the events and activities in VMs, while trying to prevent attacks without knowing what type of data is being transmitted between VMs or VMs and hypervisor.

### A. Description of Proposed Architecture

Generally, encryption is used by most of users and it is not possible to ask users not to encrypt their data. In my proposed architecture, there are not any requirements to reveal user data or encryption key to cloud providers. I have also added some new features to increase security performance in virtualization technology such as security and reliability monitoring units (VSEM and VREM). HSEM and HREM are the main components of the security system, and all the other parts of the security system communicate with them, but HSEM decides if the VM is an attacker or a victim. Actually, HSEM receives behavioral information from VSEM and HREM and never collects any information itself. In addition, HSEM notifies the hypervisor about which VM is under Level-2 monitoring in order to set service limits until the status is determined. Figure 2 illustrates the new secure architecture and the new units in VMs level, VSEM and VREM, which is available for all VMs (and also in Management VM) In addition, There are two other new units, HSEM and HREM, which is available in the hypervisor level. VSEM and VREM consume low resources of the VM, but they help to secure VMs against attacks.

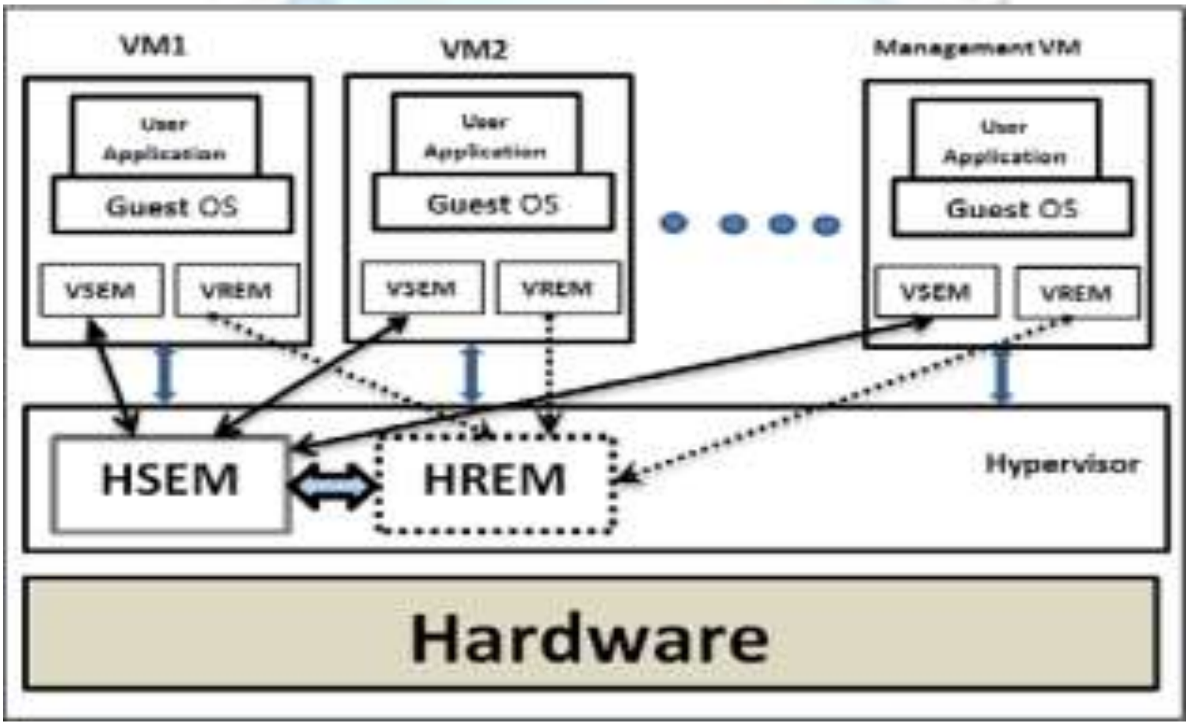


**Fig. 2: Architecture of secured virtualization**

### B. VM Security Monitor (VSEM)

There is a VSEM within every VM that is running in a virtual environment. These monitors acts as sensors, but are different from sensors. In fact, VSEM is a two-level controller and behavior recorder in the cloud system that helps HSEM identify attacks and malicious behavior with less processing. VSEM monitors the security-related behaviors of VMs and reports them to HSEM. Because there are a large number of transmissions in cloud, and sending all of them to HSEM consumes a lot of bandwidth and processing resources, which can affect general hypervisor activity, some tasks were done by VSEMs in VMs such as collecting information that is asked by HSEM. In addition, because users don't want to consume their resources, which they paid for it, VSEMs have two levels of monitoring that consume more resource only when it is necessary. Actually, each level of VSEM is monitored almost the same events but at different detail levels.

**1) Level 1**

In this level, the VSEMs monitor their own VMs. In this level VSEM collects of the source and destination addresses which are in head of data, number of unsuccessful and successful tries in sending data, and number of requests that were sent to the hypervisor. At this level, VSEM, according to the brief history of the VM which provided by HSEM, looks for anomaly behavior (HSEM has had history of VMs in more details). For instance, the system identifies the VM as a potential attacker or victim if the number of service requests from the hypervisor is higher than average based on the history of requests of the VM. If abnormal behavior is detected, or the type of sending data and unsuccessful tries increase above that threshold (according to history of the VM), then VSEM switches to Level 2 and also notify HSEM about this switching in order to HSEM investigates the VM for finding malicious activities.

**2) Level 2**

In this level, the VSEM monitors and captures the activity of the VM in more detail, such as VM's special request from the hypervisor, details of requested resources (e.g. the number of requests), and the destination transmitted packets (to recognize if it is in the same provider's environment or outside). In this mode VSEM notifies HSEM about the level of monitoring in the VM. According to this notification, the hypervisor set activity limits in types of activities until HSEM learns that the VM is not an attacker or victim. At this level, HSEM makes a request from VREM about the reliability status of the VM, including the workload status and how many times the VM workload was close to the maximum capacity of the VM.

### C. VM Reliability Monitor (VREM)

VREM monitors reliability-related parameters, such as workload, and notifies the load-balancer (within the hypervisor) about the parameter results. VREM is also used for security purposes. The VREM will send useful information such as workload status to HREM and requests the status of the VM from HSEM, and then it decides whether to give the VM more resources. Actually, if the VM requests as many resources as it can (that is different behavior according to its usage history), it may signify an overflow attack victim. Therefore, proposed HREM can detect overflow attacks and notify the HSEM about it.

## Conclusions

Cloud computing helps IT enterprises use various techniques to optimize and secure application performance in a cost-effective manner. A cloud-?asd application is based on network appliance software, with Its operating system, running in a virtual machine In a virtualized environment. A virtual appliance relieve some of the notable management issues in enterprises because most of the maintenance, software updates, configuration and other management tasks that they are done by cloud provider which responsible for them. But this suggestive way for decentralized application and access every time and everywhere to data, occasion and introduce new set of challenges and security problems that must consider before transfer data to a cloud environment. Additionally, just because the software can run in a Virtual machine does not mean that it performs well in cloud environment necessarily. Thereupon, in cloud there are risks and hidden costs in managing cloud compliance. The key to successful cloud computing initiatives is achieving a balance between the business benefits and the hidden potential risks which can impact efficacy. These issues which discussed in this paper are the main reasons that cause many enterprises which have a plane to migrate to cloud prefer using cloud for less sensitive data and store important data in their own local machines. Eventually, Whilst Cloud computing is an applicable and interesting technology that introduce in the IT industry; It doesn't mean that all business IT needs to move to cloud. In addition, As a result, Moving toward cloud computing require to consider several parameters and most important of them is security.

## References

[1]. I. Stoica, D. Adkins, S. Zhuang, S. Shenker, and S. Surana, Internet Indirection Infrastructure. In ACM SIGCOMM, 2002.

[2]. F. Hao, T.V. Lakshman, S. Mukherjee, and H. Song, Enhancing Dynamic Cloud-based Services using Network Virtualization, In VISA, 2009.

[3]. C. Guo, G. Lu, D. Li, H. Wu, X. Zhang, Y. Shi, C. Tian, Y. Zhang, and S. Lu, BCube: A High Performance, Server-centric Network Architecture for Modular Data Centers. In ACM SIGCOMM, 2009.

[4]. N. Farrington, E. Rubow, and A. Vahdat, Scaling Data Center Switches Using Commodity Silicon and Optics. In ACM SIGCOMM, 2008.

[5]. R. Mysore, A. Pamboris, N. Farrington, N. Huang, P. Miri, S. Radhakrishnan, V. Subramanya, and A. Vahdat, PortLand: A Scalable Fault-Tolerant Layer 2 Data Center Network Fabric. In ACM SIGCOMM, 2009.

[6]. J. Touch, and R. Perlman, RFC 5556: Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement. http://www.ietf.org, 2009.

[7]. C. Guo, H. Wu, K. Tan, L. Shi, Y. Zhang, and S. Lu, DCell: A Scalable and Fault-Tolerant Network Structure for Data Centers. In ACM SIGCOMM, 2008.

[8]. T. Wood, P. Shenoy, K.K. Ramakrishnan, and J. Merwe, The Case for Enterprise-Ready Virtual Private Clouds. In Hot Cloud, 2009.

[9]. T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. In CCS, 2009.

[10]. A. Greenberg, J. Hamilton, N. Jain, S. Kandula, C. Kim, P. Lahiri, D. Maltz, P. Patel, S. Sengupta, VL2: A Scalable and Flexible Data Center Network. In ACM SIGCOMM, 2009.