ISSN:0975-9646

Survey on Security Issues and Problems in Cloud Computing Virtual Machines

Shwetha S

M Tech(CSE),
Channabasaveshwara Institute Of Technology,
Tumkur , Karnataka, India

***Abstract*—This paper presents a complete study on the security issues and problems in cloud computing virtual machines. And also introduces a virtualized cloud infrastructure without the virtualization.**

***Keywords*— cloud computing; cloud security; multi-tenancy, Hypervisor, virtualization , NoHype.**

I. INTRODUCTION

Cloud computing depends heavily on virtualization. Virtualization technology has developed promptly because of the rapid decrease in hardware cost and increase in hardware computing power. A Hypervisor between the hardware and the OS enables multiple virtual machine to run on top of a single physical machine. The Hypervisor diaries and ships the physical resources to the individual VMs as needed,and they appear as a isolated computers to a end user. Cloud computing provides different strata of computing utilities through three main service models: software as a service(SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). Virtualization provides on-demand resource provisioning and multi-tenancy and we also say virtualization as a heart of computer technology. Virtual machine can be defined as " a machine which is proficient ,sequestered duplication of a given physical machine." Cloud computing adopt virtualization technique due to1) Segregation and safety in modern systems. 2)The failures in safety and consistency of standard OS. 3)The sharing of a single computer among multitenant, and 4)The dramatic increases in infrequent speed of processors, which makes the overhead of VMs more acceptable[1]. The use of hypervisors say how to draw virtual resources to physical resources. They are smaller than our traditional operating systems. Virtual machines and their images are provided by the service module IaaS . And the number of VM's running can shrink or grow a given instance. At SaaS the security is provided to isolated users data. Example of these VM are Xen, KVM, Denali.

II. CLOUD COMPUTING SECURITY ARCHITECTURE

Security is provided to all three service layers (PaaS,SaaS,IaaS) .Each layer have their own security level and security management.

Security architecture has three layers:Traditional transport layer, cloud computing layer and requirements and application-driven layer. Cloud computing layer is divided into two parts: technical security module and non-technical security module. In the technical security module there are functional service modules like SaaS , PaaS and IaaS etc. and service interactions security modules. The prior ensure cloud services and the latter promise the safe of the cloud services. Non-technical security module includes laws and regulations, management system, education and training, security policy and safety norms, which is the safety aids modules[2].The security for cloud computing is provided at four layers first is authentication security, secondly it is a file encryption , third is for privacy and last but not the least is fast file upturn. All the four layers carry out their duties to provide a highly secured data in cloud computing. Since cloud computing support virtualization and location independent data storage capacity. Security of highly confidential data is more important.

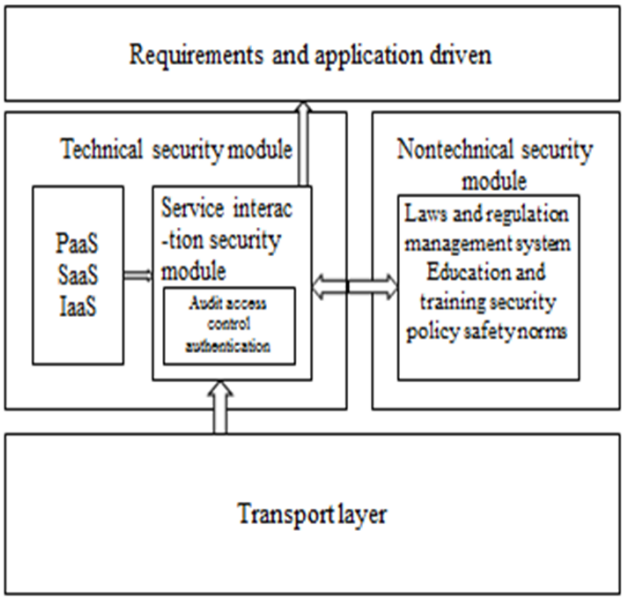

Fig 1 (from[2]) security modules in could computing

A. How security can be improved through some agents

Securing data in cloud is a complicated and serious issue. Cloud service provider make their customer data completely isolated from other user data and also they agree upon some SLA. Here let us introduce agents into the cloud to increase the security .Agent's features are sovereignty, responsivness, initiative, social etc.

1)Confirmation agent/ authentication agent: Here agents are responsible to recognize an validate users,and they provide a digital certificates through which they can manage access permission to the end user.

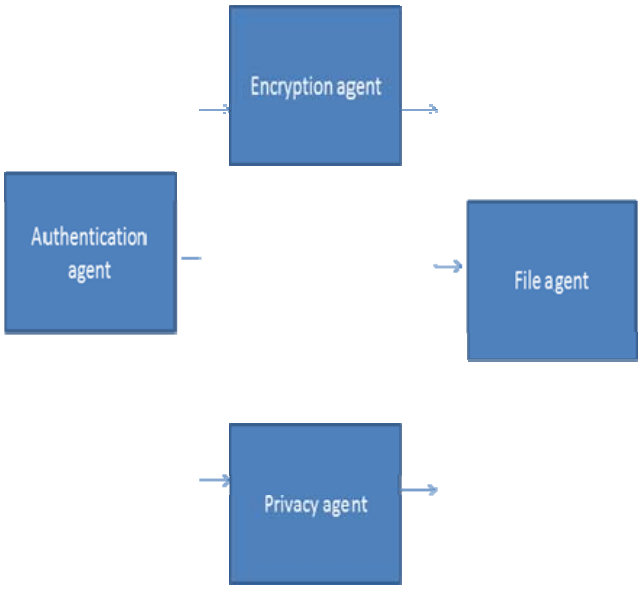

Fig 2 agents protected security module

2) *Encryption agent:* Algorithms used for encryption are AES or Rijndael . Since cloud support multi-tenancy . Confidentiality should be achieved through this enryption agents. These agents uses many symmetric or asymmetric enryption algorithm.

3)*Privacy agents:* Protecting user's data is a job of privacy agents.So privacy agent maintain users access record and they are secured even the encryption key is taken by some attacker.

4)*File agents:* Cloud contain multi users data. Each data should be isolated from one another. And they follow a method of distributed data center where customers data are stored in multiple places so that even if any disaster occur the data is secured in one or more places. If any updates are done to a given data they should be replicted in all data.

III. SECURITY CHALLENGES FACED BY VIRTUAL MACHINES

Widely used benchmarks for evaluating IT security are Confidentiality, integrity, availability, privacy, trust and audit.

1)*Confidentiality*: Confidentiality is provided to all the three service layers of cloud. Confidentiality refers to only consented users having the permission to access secure data. Confidentiality is to guarantee that user data which resides in the cloud cannot be accessed by unauthorized party. Using web browser over internet a customer or end user can access SaaS .The users data and network should be protected and isolated in transit so that none of the eavesdrop can access through the secured data. PaaS provide platform for developing applications and web services through a very highly secured isolated platform. IaaS support multi-tenancy where virtual resources are hired as per the need from a single physical infrastructure.

2)*Integrity*:Integrity mean resources can only be modified by the authorized parties in an authorized ways. Integrity is associated with any of them i.e hardware,software, data . Data is protected from unauthorized modification .Data stored in a cloud are encrypted and they follow up the ACID properties of cloud and made them location transparent. In cloud computing, the cloud provider ensure the reliable and correct operation of the cloud system and meet its Service Level Agreements (SLAs). Once again data integrity is provided in all the three service layers. In SaaS we need to protect the data which is in transit and data storage is integrated and network traffic is controlled. In PaaS and IaaS platform is integrated and file are configured so that attackers get less chances to get through the file and platform through which SaaS data can be easily trapped.

3)*Availability*:Availability refers to the property that data in a system being accessible and used upon demand by an authorized entity. The main goal of availability is to make data available all the time to its user at any place and time. The data,software and hardware are available to the authenticate user on demand and they charge their users for what they use.Data is made available even after the denial of service attack and natural disasters.

4)*Privacy*:Privacy is an important issue for cloud computing. By migrating workloads to a shared multi-tenant infrastructure, customers' private information faces increased risk of potential unauthorized access and exposure. Cloud providers must assure their customers and provide a high degree of transparency into their operations and privacy assurance. Privacy protection mechanisms must be embedded in all security solutions [3].Cloud service providers need to convince their customers that their cloud provide a high degree of isolated data and they should guarantee that their data is secured and confidential .Well privacy in public cloud is more important than in private cloud , private clouds are maintained and developed with in the organization and data is accessible only to people of the particular organization.Where in public cloud since they provide a multi-tenancy the are more vulnerable to the attacks . And there is a chances of data being intruded .

5)*Trust*: Here a cloud provider need to convince his customers saying them that their cloud provide a high security for customers data. Since customers depend on providers for their data security . Much care should be taken by the cloud computing provider by capturing efficient parameters required to build the trust between them.

6)*Audit*: The access is observed and traced to make sure that there will be no security errors in the system. It also will help assessors to verify the fulfillment to different access control policies, intermittent auditing and reporting. Assessing is the process of reviewing and Probing the authorization and authentication records in order to check the security standards and policies are guaranteed. Also, it will aid in detecting any system faults. Consistent, secure and tamper-proof log collection is necessary.Depending on the type of access to cloud system, actions of the users like administrators are recorded each and every time they access the resources.

IV. CLASSIFYING VIRTUALIZATION

Various kinds of virtualization are

1)*Process virtualization*: This creates an application without concerning about the OS it runs upon . By virtualizing this layer it provides an interface between an application and the underlying system. JVM is an example for process virtualization.

2)*Server virtualization*: This allow many OSes to run on a isolated physical machine.Here, the virtualization is applied to the hardware.

3)*Network virtualization*:Virtualizing this layer enables the interconnection of two or more different private networks through internet and allow two or more local network to share same physical infrastructure. Examples VPN and VLN.

4)*Storage virtualization*: SANs (Storage Area Networks) fall into this category[4].

A. *Hypervisors*

As defined in the introduction part Hypervisors are used to map virtual resources to physical resources. These hypervisor's are also called as VMM(Virtual Machine Monitor) which are smaller than our traditional OSes .The hypervisors are two types Type1:-Type 1 hypervisors are installed directly on the host to control the caller(guest) operating system. These caller OS runs one level above the hypervisor layer. Type 2:- This type of the hypervisors are installed above the local operating systems and they run at level three and the caller OS runs at level four .i.e above the given hypervisor.

B. *How To Find The Hypervisor Environment?*

Excluding the paravirtualization. The virtualizaton technique provide the caller OS with an identical replica of a real system. To detect whether there is a hypervisor running underneath the OS. Such techniques are useful for both attackers and defenders. An attacker can check if the targeted system is virtualized and acts accordingly. On the other hand, a user willing to check the integrity of his machine can check for the presence of a hypervisor installed against his OS. First, a hypervisor can be detected by checking the execution time of some instructions because the processing of such instructions by the VMM requires more time than when the system is not virtualized.

Secondly , the measurements of the time needed to access the Translation Lookaside Buffers (TLB): once those buffers have been filled with some known data. By calling the PROCESSORID instruction enables the cleaning of at least one portion of the TLB if a Hypervisor trapped it. Then, by comparing the access times to the TLB measured before and after calling PROCESSORID, one can establish the presence of a hypervisor. Once a hypervisors are correctly identified, an attacker can adapt his attack's state of affairs to the vulnerabilities known as characteristic of the hypervisors. These techniques identify those VM that match with characteristics specified by the intruder and make them as a target machine to get access through the hypervisors. Once the intruder get access to his targeted machine it is difficult to identify which caller OS is an intruder among a infinite set of caller OS running under a single cloud[4].

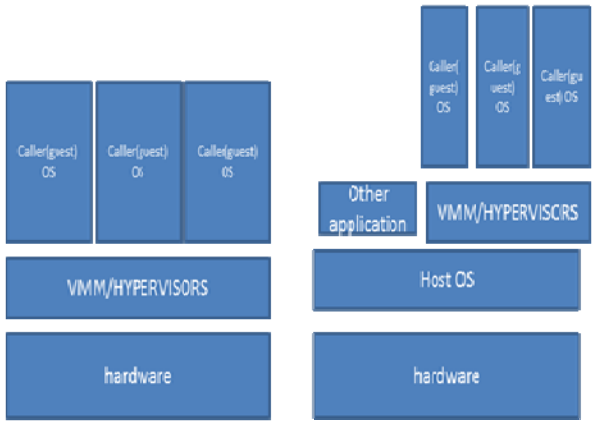

Fig 3 (a) type 1 (b) type 2

C. *How Virtual Machines Are Accurately Targeted By The Intruders*

In this paragraph, we will focus on the works done by Ristenpart et al. [5]. Their research work consists in identifying techniques to ensure a coresidence in a public cloud . This means that the authors are able to obtain a VM that is hosted on the same real host as another VM they want to attack.Thanks to this co-residence, they are able to monitor some activities of the targeted VM through a covert channel. Let us note that, in these experiments, only "valid" tools were used and no modification of the targeted systems has been done. The authors started by establishing a map of the cloud: they examined how the IPs were distributed according to the characteristics of the corresponding VMs (number of cores, storage capacity,). Then, they identified several techniques for checking the co-residence between an attacker's VM and his target, first through a network analysis (if the first node is the same, or if the IPs are within a certain range, they are co-resident), then by measuring the host activity. To do so, they compared the time required for reading a given portion of the memory before and during an intense activity imposed to the target (by sending multiple requests to the targeted server). Results of this experiment are shown in figure 4. The target is a web server to which multiple HTTP get requests were periodically sent. In the first two graphs, there is a clear distinction between the activity recorded during the HTTP gets and the "standard" activity ("No HTTP gets"): the two machines are co-resident. In the third graph, no distinction can be made: two machines are not resident on the same real host. Once that co-residence is confirmed, an attacker can obtain more information about the target activities with a similar method (by monitoring the host activity without interacting with the target) or try to take over it by other means.

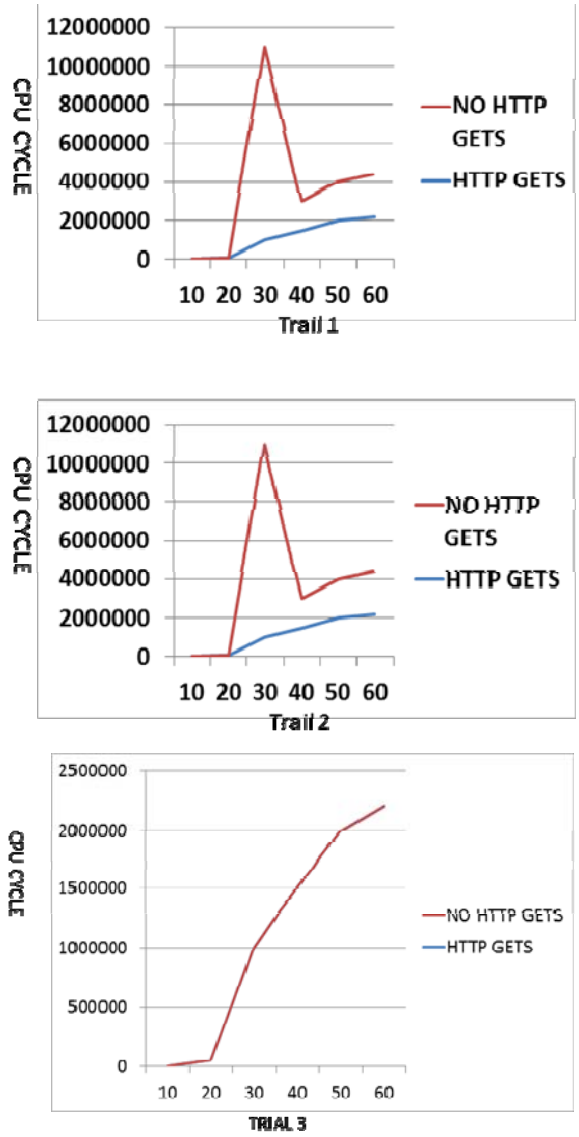

Fig 4 Co-residence in a Cloud .

D. *Vulnerabilities In Cloud Security Due To Virtualization*

Virtualization is a core of cloud computing where they provide multi tenancy. Multiple isolated virtual machines can run on a single physical machine with the help of virtualization.the hypervisor or the VMM is a software which acts as an intermediate between VM and a local host. They also schedule the underneath physical resources among a VMs . The resource allocated to one VM can be used by other VMs but cloud service provider should provide the security to each isolated data ensuring that no data has been leaked when sharing the resources.

There are certain vulnerabilities caused by virtualization they are[6]:

i)*VM Hopping* :An intruder residing in any of the VM can get access to any other VM. The intruder can then alter, delete the data stored in victims VM .The main reason for this type of vulnerabilities is due to VM s running on same host . Here the attacker get the IP address of victim VM before intruding . If suppose an intruder attacks PaaS and IaaS service layers then it is easy to alter the data and application present in SaaS. PaaS and IaaS are the foundation layer for SaaS.

ii) *VM Diversity:* Virtualization allow the users to create VMs but protecting the VMs from an attacker is a risky task.Since it support many VMs supporting and maintaining a wide range of OS is perilous. Cloud customer service provider should provide different level of SLAs to different VMs user due to the portable nature of the cloud . In IaaS the service provider provide security and vigor to the services they provide and the user should share the responsibility of updating the data and the OS . Both the service provider and the user should agree up with certain legal obligation.

iii) *VM denial of service:*Virtualization lets multiple VMs share physical resources, such as CPU, memory disk, and network bandwidth. A denial-of-service (DoS) attack in virtualization occurs when one VM occupies all the available physical resources such that the hypervisor can't support more VMs, and availability is imperiled. The best approach to preventing a DoS attack is to limit resource allocation using proper configurations. In cloud computing, DoS attacks could still occur, but having service providers set adequate configurations to restrict the resources allocated to the VMs reduces their probability. In addition, it's beneficial to configuration management to have the SLA clearly define service provider and user responsibilities[6].

iv)VM Mobility: The data of VMs virtual disks are stored as files and VMs can be moved or copied from one host to another over the network.One can store devices without physically pilfering a hard drive. VM mobility provides quick deployment but could lead to protection problems. In IaaS , cloud service provider offer hardware and resources to the users to develop one's own computing VMs. SLA complexities due to VM Mobility can be reduced by clearly specifying the shared responsibility of the service provider and the users.

V . Cloud Infrastructure Without Virtualization

There are many clients (customers) and servers, and management of the provided infrastructure is highly robotic. The cloud providers use multi-tenancy where multiple end users use share a single server through virtualization. This multi-tenancy is a source to which a security should be provided because due to multi-tenancy intruders can get a direct access to the server where targeted VMs is currently running. Once the access to victim VM is possible then it is easy to get the encryption keys ,data and even possible to modify the underlying hardware and software. Rather than making virtualization layer more secured we move on to a architecture which provide you virtualized cloud communications without the virtualization.This architecture is also called as No-Hype architecture which gives an entire solution by combining processor technology,I/O technology and software[7]. Here we remove the virtualization layer by providing No-Hype. This mainly revolve around the isolation of resources. When ever any guest VM need to access the cloud data , this no-hype provide entire resource to that particular guest VM, and the guest machine have full contol over the resource through its implementation on the physical machine.

A. *Characteristics of NoHype Architecture*

*i) CPU: One VM per core:*Each core can run only one VM. That is, cores are not shared among different guest VMs, they removes the need for the active VM scheduling done by the hypervisor. Since we are in the generation of producing multi-core. VMs per server depends on the core which reside in the server. The cloud infrastructure is dynamic in nature and the need for VMs are scaled up or down according to the users and application needs.

ii) Memory: Here physical memory is partitioned by giving each caller OS a view of memory where every caller OS will have a dedicated guest physical memory on the host system. The mapping of guest physical memory to actual physical memory is done with the help of hardware.

iii)Devices:Here each caller OS is assigned its own physical device and are directly accessed . Of course, this relies on the assumption that there are enough devices to assign at least one per virtual machine. We believe that the view of multiple physical devices should be realized by the device itself supporting virtualization that is, the device would be a single physical device, but tell the system that it is n separate devices. Each VM will interact only with the virtual device(s) assigned to it. As seen in Figure 6, a virtual device can have one or more queues dedicated to it. This forms the interface that is seen by the associated VM. The primary devices needed in a cloud computing scenario are the network interface card (NIC) and the disk. Other devices, such as graphics processing units (GPUs) could also be virtualized, thus removing a need for having N separate devices [7].

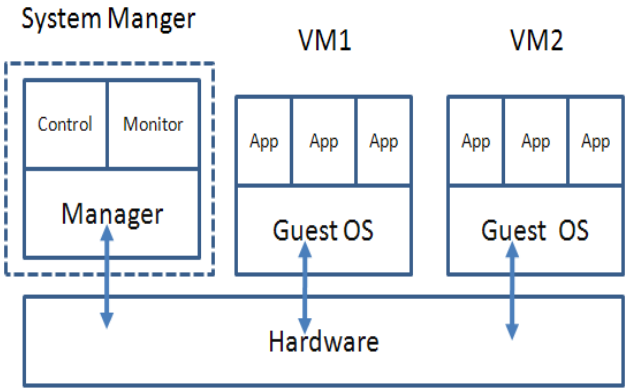

Fig 5 (from fig 1[7])A server in the NoHype Architecture .

B. *The NoHype System Architecture*

This architecture is made possible by using hardware assisted virtualization and putting several constraints on the conditions of virtualization: each virtual machine is linked to one unique processor core, the portion of memory allowed to it is fixed and managed by the hardware and each (virtual) device is dedicated to only one VM. Figure 6 gives an overview of NoHype implementation. MMC stands for Multi-core Memory Controller. It is the device dedicated to managing the allocation of memory to each core. The system manager (on the left) also runs on one dedicated core, which is the only one allowed to send IPIs (Inter Processor Interrupts) to other cores, enabling the startup, shutdown or migration of a VM on them. For example, to start a VM, the system manager prepares the required resources and sends an IPI to the core on which the VM is supposed to run. This core runs a program responsible for configuring it (by mapping the allocated resources) then starts theVM image. The effective virtualization of the caller OS is realized by a tiny hypervisor, called core manager . The system manager is then able to communicate exclusively with the core managers and only to trigger the migration or termination of a VM.

However, due to its design, NoHype loses some features offered by more traditional virtual machine managers, such as the ability to share resources (devices, memory buffers) between several VMs[4]. As seen in Figure 5, a virtual device can have one or more queues dedicated to it.

This forms the interface that is seen by the associated VM. The primary devices needed in a cloud computing scenario are the network interface card (NIC) and the disk. Other devices, such as graphics processing units (GPUs) could also be virtualized, thus removing a need for having N separate devices[7].

C . *NoHype Security Benefits*

In NoHype architecture, customers are provided with enough security to run their VMs in their own virtualized infrastructure. To achieve security for customers VMs ,no VM should affect the other VMs ,should not access data and software of other VMs and confidential informations are learnt through side channels. There we follow up with the benefits of NoHype security:

Availability: Availability can be attacked in one of three ways in current hypervisor-based virtualization architectures–(i) altering the hypervisor's scheduling of VMs, (ii) interrupting a core running a VM, or (iii) performing extraordinary amounts of memory or I/O reads/writes to gain a disproportionate share of the bus and therefore affect the performance of another VM. By dedicating a core to a single VM and removing the hypervisor from making any scheduling decisions, we eliminate the first attack .To eliminate the second attack we do hardware Masking for inter-processor and device interrupts, there is no possible way to interrupt another VM. By limiting the access to I/O and memory one can eliminate third attack. with the NoHype architecture, a VM has no ability to disrupt the execution of another VM.

Confidentiality/integrity of data and software : In order to modify or inspect another VM's software or data, one would need to have access to either registers or physical memory. Since cores are not shared and since there is no hypervisor that runs during the entire lifetime of the virtual machine, there is no possible way to access the registers. Since the NoHype architecture enforces memory accesses in hardware, the only way a VM could access physical memory outside of the assigned range would be to alter the tables specifying the mapping of guest physical addresses to host physical addresses. To do so would require compromising the system manager software and altering the code performing the start/stop functions. This would first require compromising the cloud manager, which we assume is trusted, as the system manager only interacts

with the cloud manager and the core managers, and is isolated from the guest VMs.

Side-channels: Side-channels exist whenever resources are shared among multiple pieces of software side-channels are typically based on the timing of operations(e.g., hits in caches are shorter than misses, so one can determine if a particular cache line was accessed by timing an access to a specific memory location).

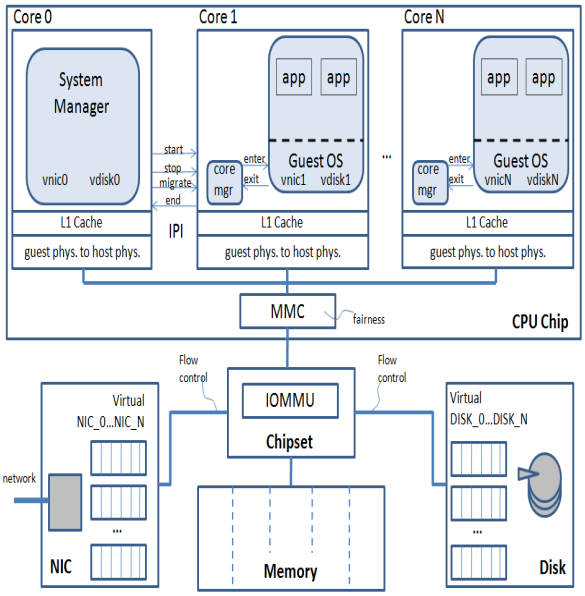

Fig6 The NoHype system Architecture

VI . CONCLUSION

While cloud computing has a great promise of security to the users data. Some time the users data may be tampered by external intruders . Since cloud provide location independent data and also allow multi-tenancy, security is the major issue here. Virtualization is a concept to which cloud tightly stick on and there is a high risk of vulnerabilities due to this hypervisors. To eliminate these vulnerabilities in the virtualized environment we introduced a NoHype architecture where high security is provided to each isolated data without any virtualization.

REFERENCES

[1] John L Hennessy and David A. Patterson"Computer architecture A Quantitavie Approach" ELSEVIER 2010

[2] "Applying agents to data security in cloud computing" Feng-qing Zhang, Dian-Yuan Han,2012 International Conference On Computer Science and Information Processing.

[3] HuagloryTianfield,"Security Issues In Cloud Computing",2012 IEEE International Conference on Systems,Man and Cybernetics.

[4] Ivan Studnia,Eric Alata,Yves Deswarte,VincentNicomette"Survey Of Security Problems In Cloud ComputinVirtual Machines",2012 December.

[5] Ristenpart, T., Tromer, E., Shacham, H., Savage, S.: Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security. pp. 199–212. ACM (2009)

[6] Hsiin-YiTsai, Melanie Siebenhaar and Andre Miede"Threat As A Service"IT Pro January/Febuary 2012.

[7] Eric Keller ,Jakub Szefer,"NoHype:Virtualized Cloud Infrastructure Without The Virtualization"Princeton University,USA,June 2010.

[8] John Viega"Cloud Computing And the Common Man",IEEE computer society 2009.