ABSTRACT

Nowadays, almost every IT companies tend to use virtual machines as platform for their IT services instead of physically separated machines. This simplifies the management of the IT infrastructure and also reduces the hardware costs. However its popularity in contrast, not automatically increases its security. Virtual environment faces the same security threat as the non-virtualized. And there is also less solution for virtualized threats then non-virtualized. Hypervisor manages the virtual machines and cloud systems. Unauthorized access to a hypervisor might mean compromise of complete data. There are different kinds of attacks that can compromise security of hypervisor providing full access to malicious users such as Session Hijacking, Flooding attack and Malware injections. To address these attacks, in this paper we propose a highly secured framework for hypervisor. In particular, we enhance session hijack avoidance algorithm by using clock SYNC and query/value pairs and encrypt the data exchange to avoid other major problem i.e. data monitoring.

INDEX TERMS—Cloud computing, Virtualization, Hypervisor, Security Framework

I. INTRODUCTION

Nowadays almost every IT companies rely on cloud computing. It consider as a next big thing in IT world. Cloud computing stands on two key concepts abstraction and virtualization and by help of these two it provide as services and applications that accessed by standard internet and network protocols which are running over a distributed network using virtualized resources. Cloud computing is turning the manner by which people use computers along with how networked services are run. The cloud service provider is capable to dynamically style existing infrastructure to encounter the present request from cloud infrastructure provider by leasing infrastructure. The service provider fixes this via applying virtualization where virtual machines from numerous clients share the similar physical server.

Cloud Computing is an ideal for on-demand and allowing suitable network access shared resource group (e.g., storage, networks, applications, servers, and services) that can be quickly provisioned and free with very little super vision effort or provision provider interaction. Numerous organization acquiring cloud computing as it grant them to right to use services, applications and resource over the network or Internet on an “as-required” or “per-usage” basis. This takes certain beneficial effect on price and agility for the IT department. According to survey of January 2011 by Unisys, approximately half of U.S. companies think cloud computing as the top IT priority. Cloud computing has many advantages such as save money of IT departments and increase flexibility.

Virtualization has major role in bringing the cloud computing era. It turned the thinking from physical to logical, rather than running IT resource as separate physical entity, it treats it as logical resources. It basically refers to the abstraction of computer resources. To deliver virtualization, hypervisor turn into the important software, which is also recognized as Virtual Machine Monitor (VMM). Its main responsibility is to observe the Virtual Machines (VMs) that are working on upper layer of it.

Services of cloud computing rely on sharing so security in these system is a major worry and virtualization’s security dependent on security of individual component (hypervisor, host operating system, guest OS, storage and applications).

In this paper we discuss the hypervisor and security attacks. In next section, related work is discussed. In section III hypervisor its type, commercial products and benefits are described. In section IV security and attacks are mentioned and section V problem statement then followed section describes about security framework for hypervisor and at last section conclusion and future is presented.

II. RELATED WORK

Various research is done on security and cloud it may related to its storage, users, virtual machines, accountability, host operating system, cloud applications and hypervisor.

Nancy Arya they we can expect to see a lot of security incidents and new kinds of vulnerabilities around it within the decades to come. They depicted some
crucial and well known security attacks malware injection, flooding attack, eavesdropping and session hijacking attack of different security notions that can be possible on hypervisor. This paper also proposed some potential solutions and precautions to maintain security. To increase the security performance parameters such as reliability and security Farzad Sabahi introduce two new components i.e. HSEM & HREM which related to security and reliability of the hypervisor. Hyperwall architecture is introduced to provide protection to guest VM by a malicious hypervisor and this technique reduces runtime overhead and impact on memory performance. D.A.B Fernande et al. do survey on security issues n cloud environment his survey determine various attacks on cloud such as attacks based on memory, guest machine, host machines, hypervisor, protocols, internet, accountability, and availability. Through there one can easily understand the various possible attacks that can be done on cloud environment.

III. BENEFITS AND TYPES OF HYPERVISOR

Hypervisor is a thin software layer that provides abstraction of hardware to the operating system by allowing multiple operating system or multiple instances of the same operating system, termed as guests, to run on a host computer. There are numerous companies in cloud computing market, which are offering this technology like Red Hat, VMware, xen.org, Microsoft etc.

1. BENEFITS OF HYPERVISOR

(a) Isolation: -It assurances that software running on one of the virtual machine’s doesn’t affect the remaining virtual machines in any kind of way. Data of one virtual machine by default not is accessible by any other virtual machine. For example malicious software within one particular VM can only affect that machine no other VMs, hypervisor or physical hardware.

(b) Small codebase: - Hypervisor have error-free code because of smaller and less complex codebase than modern operating system. So its security ensure is much easier as compared to O.S.

(c) Moving security out of the VM:- It offers the possibility of moving the security mechanism out of the OS. For example if VM compromised even then protection mechanism such as anti-virus provides protection to the system.

2. TYPES OF HYPERVISOR

VMM can be classified in two types: Type I (also known as bare-metal) and type II (also known as hosted) [1]. Type I Hypervisor, which is too recognized as “native hypervisor” or “bare metal” as it directly [1], works on the upper of the underlying hardware as presented in Fig. 1. In this situation as there is no operating system working below it, VMM is a minor code whose concern is to plan and allot system entity to VMs. Examples of Native VMM are Xen and VMware ESX. In this situation the VMM make available device drivers that to directly access the underlying hardware guest OS uses.

![Type I Hypervisor](image1)

Type II Hypervisor (It is also familiar as hosted VMM), in this hypervisor runs as an application in a usual operating system that is known as host operating system [10]. The host OS it treats it as any other process; does not have any knowledge about Type II VMM. On behalf of guest OS it performs I/O operations. The I/O request that is trick by host OS is issues by guest OS that in order send to device driver that perform I/O, via host OS the finished I/O request is again route back to guest OS.

![Type II Hypervisor](image2)

3. COMMERCIAL PRODUCTS

KVM, VMware ESX, Microsoft Hyper-V, XEN are various dominant hypervisor [1] use in these days.

KVM (Kernel-based Virtual Machine): that is employed as a loadable kernel module that changes
the Linux kernel into Type-I (bare-metal hypervisor). Without the hardware virtualization extensions like AMD and Intel VT-X, KVM does not run on CPUs [10]. It consists of two building blocks:

(a)Kvm.ko: core virtualization infrastructure is provided by this loadable kernel module. (b)Kvm-[intel|amd].ko: This component converts Linux kernel into type-I hypervisor. It is a loadable kernel module for processor specific module for AMD or Intel.

XEN: This hypervisor is a software layer which directly assembles on the hardware that permits multiple virtual guest OS to course concurrently in an efficient and secure manner [10]. Its main responsibility towards core hypervisor activities such as memory virtualization, CPU, scheduling of virtual machine and power management [1]. In this there are two domains DomU and Dom0. The Dom0 perform special right because of its special privilege, it modified Linux OS and can access the physical resources and also interact with other VMs that run on xen.

HYPER-V: It virtualization system’s hypervisor for x86-64 architecture [1]. The chief duty of hypervisor is to run isolated execution environment that is identified as partition. In which operating system execute that logical unit is known as partition. Windows server 2008 running by one root or parent partition that one hypervisor must have, which then create sub/child partition through hyper call application programming interface that host the guest operating system [10].

VMware ESX: The first product of VMware was VMware workstation become first product of VMware successful for desktop virtualization. The basic of VMware ESX has three major modules which are physical host server, VMkernel and console operating system whose crucial responsible for memory allocation, regulating CPU affinity, and oversubscription, network bandwidth throttling and I/O bandwidth control [10][1].

IV. SECURITY AND ATTACKS

Security is the major problem in virtualized environment. The security of a virtualization is deeply dependent on the hypervisor. Hypervisor is the single point of failure. So, the hypervisor too needs to be wisely monitored for signs of compromise. All the virtual machines can be simply copied and changed, if the managing environment is compromised. Furthermore, because of the higher privilege level of the management operating system attacks from the management environment simply bypass the security mechanisms existing in guest virtual machines. Hypervisor can be unsecure for the guest virtual machines. There can be two type of attack that mainly done on hypervisor: client-server architecture attacks and web-browser based attacks. In this paper we are focusing on web-based attacks.

Cloud infrastructures are not only relying on hardware where user’s data stores and processed but also the path over which it is transmitted. Large number of packets are sent from sender to destination in cloud scenario through number of third-party devices and internet is transmission medium for this transmission so one should assume it’s inherit problems. Cloud services are needed to be managed and used over web and browser is a best application to provide management interface to the end user. Cloud inherit many well-known issues, such as MitM attacks, Session hijacking attacks, malware, port scanning, IP spoofing and packet sniffing.

SESSION-HIJACKING: -HTTP is stateless protocol and doesn’t guarantee delivery so address this, there are session handling technique for web applications.Sessions hijacking basically attack of taking control over valid user’s session of a web application and after gaining successful access to session generating authentication session ID. In session-hijacking, exploit the valid computer session to achieve the illegal access to service or information in a computer system. It is utilized to refer to the stealing of a cookie which is used to validate a user to a remote server. Thus, Session id should be regenerate frequently as a precaution in the small time duration after a successful login. This prevents session fixation.

CLOUD MALWARE-INJECTION ATTACKS: - In this attack an opponent tries to inject malicious code or service, which appears as one of the valid instance services running in the hypervisor. The hypervisor service will suffer from eavesdropping if in case the attacker is successful. Therefore, Hypervisor should not allow vulnerable machine or malicious in its environment (template). Hypervisor should inform owner of that machine and request to block all the vulnerable ports, if any vulnerable machine or vulnerable ports is found.

MitM ATTACK: - In man-in-middle attack one attacker machine is placed in the path of communication of virtual machines, when data is exchanged between two virtual machines. This causes network traffic among the dual computers to flow over the attacker’s system, which empowers the
attacker to review all the data. Attacker drives false spoofed mails onto a receiver by using ARP spoofing. Incoming request is forward to attacker's machine port by ARP spoofing. By attacking on single virtual machine, attacker can gain access to other guest machines and host machine. So, hypervisor to detect ARP Poisoning attacks should use IDS (Intrusion Detection Systems).

Some security threat such as covert channels, explicit information flows, single point of failure and resource monitoring [2].

Covert channel occur whenever two groupshave access to a mutualvariable where one groupcan write to this variable and the other groupcan read from that shared variable [1]. It is basically a way to transmit information to other party through hidden channels which are not meant to be for communication.

Single point of failure meant to be if hypervisor will compromise then all access of all VM and their data granted to the attacker. One VM can monitor the resource usage of other VM and for instance if sensitive information such as credit card no share on clear network and intruder monitor the network so it can cause problem for user.

There various approaches for securing hypervisor or decreasing the effects of such threats are Terra, VAX VMM and sHype. These approaches provide flexibility, A1-level security requirement of ncsc and control explicit information flow respectively. Secure Hypervisor Approaches [1] define below briefly:

(a)Terra: It provide flexible architecture to run on hardware with wide range of security requirements. In this root security is provided, only creator of close-box VM can access and modify it. Remote attestation is there to check whether the host is dependable or not, which raises the security of remote application.

(b)VAX VMM: Its primary goal to meet the A1-level security requirements of NCSC. VAX hypervisor supports both MAC and DAC. In this MAC enforces Bell-La Padula model for privacy and Biba for integrity. Each subject and object classified secrecy class as well as integrity. It carefully analysed the covert channels. If user wants to access a VM he has first to authenticate himself to the VAX VMM. Then between user and server process trust path is established.

(c) sHype: Its main objective to develop a way to control the explicit information flow between VMs. It minimizes the possibilities of covert channels.

So we need to provide architecture that supports the security of hypervisor.

V. PROBLEM STATEMENT
Hypervisor manages the virtual machines and cloud systems. Unauthorized access to a hypervisor might mean compromise of complete data. There are different kinds of attacks that can compromise security of hypervisor providing full access to malicious users. The main attacks are:

1. Session Hijacking
2. Packet spoofing
3. Flooding attack
4. Malware injections

Session hijacking problem can avoid by regeneration of Session IDs after some time. Change in hypervisor session ID can be easily observed by monitoring data. This will lead compromise in security of session.

Data monitoring is another big problem that can provide unauthorized access to data being stored in cloud systems.

So we are going to enhance session hijack avoidance algorithm by using clock SYNC and query/value pairs. To avoid data monitoring we going to encrypt data exchange. And develop user access policy for enhanced data security in Cloud systems. Improve User access policies to make hypervisors more secure.

VI. FRAMEWORK FOR HYPERVISOR
In this section we discuss the methodology, algorithm and then present technique which will use to secure hypervisor from session-hijacking attack and data monitoring.

1. METHODOLOGY AND TOOLS
We start our process by setting up KVM hypervisor environment and then create cloud environment on that hypervisor environment.

Perform some security test on the environment. Then update session management algorithm by adding clock/sync to it and implement it on hypervisor. To avoid eavesdropping we apply user access policy to
the hypervisor. And at last we compare the both security system new and existing one. If results provide better security then save the results and end the process otherwise go back to session management algorithm for improve the security and perform the same process.

Methodology is ready its time to implement it.

For implementation we use

UBUNTU uses KVM as the backend virtualization and libvirt as its toolkit.

KVM it is an open-source hypervisor as discussed in section 3.3. It is more responsive and easily installs without deals with any licensing, offers more functionality (which is equivalent to VMware motion, which hit huge amount of budget in VMware) than others and there is no problem of limited set of guest operating system as in XEN hypervisor.

ECLIPSE is open-source tool. We used it to update and implement the session management algorithm and for performing various security tests.

2. TECHNIQUE

This framework prevents the browser based attack. It provides better security to the hypervisor against session hijack and data monitoring attacks. Session authentication in this framework is done by validate session by comparing time of client and server machines. It uses sever time and client date as session login credentials and the calculate time difference of both. If an attacker try to access the web application using valid session ID then access by him will denied because of unmatched time difference which is calculated when session is generated.

```java
public boolean authenticateSession(Date clientdate) {
    if (clientdate == null) {
        return false;
    } else if (cvtToGmt(Calendar.getInstance().getTime()).compareTo(cvtToGmt(clientdate)) == this.timedifference) {
        return true;
    } else {
        return false;
    }
}
```

Fig: Session authentication

It also prevents user access policy to the cloud. It provide authentication to user over the cloud so that it provide more security to cloud user and their data. Triple DES is used to encrypt the data exchange. Eavesdropping is also a main problem in cloud environment, by using this framework we can also prevent it.

```java
public static void encrypt(SecretKey key, InputStream in, OutputStream out) throws NoSuchAlgorithmException, InvalidKeyException, NoSuchPaddingException, IOException {
    Cipher cipher = Cipher.getInstance("DESede");
    cipher.init(Cipher.ENCRYPT_MODE, key);
    CipherOutputStream cos = new CipherOutputStream(out, cipher);
    byte[] buffer = new byte[2048];
    int bytesRead;
    while ((bytesRead = in.read(buffer)) != -1) {
        cos.write(buffer, 0, bytesRead);
    }
    cos.close();
}
```

Fig: Triple DES encryption

This framework will provide better results than existing techniques.

VII. CONCLUSION AND FUTURE WORK

Hypervisor is a tool that enables one or more operating system to run on the same physical hardware i.e. it enables virtualization. This paper enables researcher to wisely choose correct hypervisor based on the taxonomy proposed on this paper. This paper also provides information to evaluate the existing various hypervisor web based attacks and solutions. Research results in solution for session hijacking attack on hypervisor. When cloud provide service over web, session is generated an attacker try to access the service by capture valid session ID which is allocated to the valid user. This problem can fix by enhancing the session management algorithm by applying clock/sync technique. In which time of server and client is used as Session key or login credentials. Time difference is calculated which is used for session authentication. If time difference is matched then access granted otherwise denied. Data exchange or service provided over web can be eavesdrop by attackers so triple DES encryption is done to overcome the data monitoring problem.
Research results in providing better security for hypervisor against web-based attacks.

Future research can do various other client-server attacks and web-based attacks such as for malware injection, attacker inject malicious code or service, which appears as one of the valid instance services running in the hypervisor. Hypervisor should inform the owner to block all vulnerable ports but it may take some time and during which attack can cause damage to the hypervisor environment. So researcher needs to figure out such problems.

REFERENCES


