

**Faculty of Computing and IT**

**UNIVERSITY OF SIALKOT**

**(*Virtualization security*)**

**Submitted By: Roll No.**

**Hijab Fareed 24020103-026**

**Ayesha Shamim 24020103-027**

**Ayesha Ashfaq 24020103-028**

**Muqadas Haroon 24020103-031**

**Course: Virtual System and Services**

**Assignment: 03**

**Department: Bs-IT**

**Semester: 7th**

**Submitted To: Sir Mohsin Ali**

**Title**

1. ***Virtualization vulnerabilities, security issues, and solutions:***

***a critical study and comparison:***

* ***Key Concepts and Technologies*:**

Cloud computing is based on the concept of virtualization, a technological solution enabling n applications on one physical server . VMs need to be managed and needs VMs to run as-isolation From the hypervisor, this also is a vital part that acts as a manager for the VMs being created. There are two main hypervisor types: Type-1 (or bare metal) runs directly on the hardware and Type-2 (hosted) run inside an operating system. Otherwise popular tools to do this technology are KVM, Xen, VMware and Hyper-V. Open-source platforms, such as OpenStack or Eucalyptus are also very popular. Virtualization provides substantial capabilities, but vulnerabilities like VM escape and hyperjacking close to as frequently are hyperjacking at the same time with quite some features a big hole in your defense.

* ***Real-World Case Study:***

Let us see how to set up an IaaS infrastructure using OpenStack in a practical example, so as to help here, with deployment point. This is another interesting hack where they could be using this setup to power a company with probably dozens of virtual servers on only 1 or 2 physical machines which would help them reduce costs and make it scalable. However, if a single VM gets compromised perhaps by a misconfigured virtual firewall then an attacker can take advantage of the hypervisor to access other VMs in the cluster or in some cases, the physical host. An actual example where side-channel attack enabled co-residency detection analysis, allowed an adversary to read cryptographic keys from phisycal neighboring VMs showed how serious the threats.

* ***Performance and Security*:**

At the performance level, virtualization allows **load balancer, fault tolerance** and also **resource allocation** for example. However, this also increases a bigger **attack surface** Main risks are :

* **VM Escape:** (malware from a virtual machine escapes isolation and attacks the host)
* **Hyperjacking:** The bad actors are able to take control of the hypervisor itself, making them completely invisible to VMs.
* **Side-Channel Attacks**: CPU cache leakage, which is the most common side channel attack.
* **VM sprawl:** Untended VMs running on your environment use resources and increase exposure.

1. ***Security Aspects of Virtualization in Cloud Computing***

* **Key Concepts and Technologies:**

Let’s start with the basics: Cloud computing is like a magical buffet for IT services pick what you want, pay for what you eat, and don’t worry about the dishes (hardware). The secret sauce behind this buffet? Virtualization. It lets one physical server pretend to be many, hosting multiple Virtual Machines (VMs), each minding its own business—ideally.

The **hypervisor** is the bouncer at this party, keeping VMs apart and making sure nobody spikes the punch. There are two main flavors: **bare-metal** (directly on hardware, for serious business) and \*hosted\* (sits on top of an OS, for lighter workloads). Virtualization also relies on \*disk images\* (think: VM selfies) and **snapshots** (VM time machines).

* ***Real-world Use Case:*** **Cloud Service Providers**

Imagine you’re a company moving your business to the cloud. You rent VMs from a provider. You expect your data to be as private as your browser history (or more so). But if the provider isn’t careful, a rogue admin or a sneaky neighbor VM could peek at your data, or worse, mess with your VM’s settings.

According to the paper, 50% of cloud users lose sleep over whether their provider is up to snuff on security. And with 52% of cloud attacks targeting web applications, it’s clear the cloud isn’t all rainbows and unicorns—sometimes, it’s thunderstorms and gremlins.

***Performance or Security:***

Virtualization is like running multiple apps on your phone at once great until one app hogs all the memory and everything slows down. Cloud providers must limit how much juice each VM can use, or risk one bad apple spoiling the bunch.

**Hypervisor Attacks**: If the bouncer (hypervisor) gets tricked, an attacker can control the whole party. Attacks like **hyperjacking** or **VM escape** let a malicious VM break out and wreak havoc.

**VM Attacks:** Malware inside a VM can spy on keystrokes, steal data, or launch attacks on other VMs, especially if isolation is weak.

**Image Attacks:** Old or unnecessary VM images are like forgotten leftovers in the fridge—they can go bad and cause trouble if not cleaned up. Attackers can steal data from these images or use them to sneak into the system.

**Service Provider Risks:** If the provider’s staff or software isn’t trustworthy, your data could be exposed, altered, or deleted.

***Overview of Virtualization, Attacks, Different Case***

***Studies and Mitigations:***

* **Key Concepts and Technologies:**

In the land of IT, a lie from the mouth of virtualization: it lets us all run multiple computers (VM) in single physical machine, and all in the hand of single landlord (hypervisor to make sure no one thrown after eating more than their share)! Cloud: you can provision parts of computers (aka “servers”) with this technology and you are actually taking advantage of a stack that consists to enable hundred or more applications running on-shared-computer without one noticing how many other applicaton neighbor.

But like any apartment building, there is the possibility of an intrusion by an over curious neighbor. In virtualization space, this is the VM escape A sneaky tenant that sneaks into another unit and around the building to the landlord (hypervisor) or another unlucky tenant (VM).

* ***Real-World Case Study***

Let me introduce to you, an actual home invasion: CVE-2008-0923. Vulnerability in shared folders in vm from VMware, allowing guest VMs to read from unlisted folder on the host system (the naughty tenant who tries to peek through the landowner files by disconnecting and reconnecting a USB drive).

Attackers used advanced techniques (like p-trace system calls) to jump into root-space and execute arbitrary code, reducing a regular VM into the master key to the whole building.

Case study — More famous example : Spectre and Meltdown where CVE-2017-5753, CVE-2017-5718. These attacks went straight to the heart of the computer (CPU), conscripting it into leaking secrets from neighboring VMs.

Now, imagine someone whistling through the walls and hearing your Wi-Fi password—creepy right?

* **Performance or Security**

And while virtualization is super for efficiency — more VMs per server means fewer servers, therefore cost savings,plus flexibility because you can move virtual instances around. However, solving vulnerabilities (Spectre, Meltdown) is running things slow like putting more doors in your building that also lock. Important security updates are slow, but they often come with the price of performance and add a little rent for that extra bit of homeless people security.

VM Escape most catastrophic **single breach.** If the adversaries get past, they can:

Expose other VM data.

Alter or take over data

Unstable caregivers

Then Colossally Move laterally to destroy other portions of cloud

Here’s where attackers tend to do it in two steps:

**1.** Placement: place malware VM of the attack vector with same host physical machine as target.

**2.** Extraction Use the exploits to get out and steal data.

***Survey on Virtualization Service Providers, Security Issues, Tools and Future Trends***

* **Key Concepts and Technologies**:

Virtualization is the IT shapeshifting spell of it-world: it allows to slice one physical computer into several virtual ones that perform all tasks by themselves — a real life octopus on the computer. At its core, this tech is a major driver of cloud computing which enables more than one OS and application on a server thus letting them use it instead of paying big bucks for actual hardware.There are different types of virtualization :

**Full Virtualization:** Pretends the hardware is real so all operating systems do not have to know any better.Types:

* **Bare Metal (Type 1)** Hypervisor sits directly as straight hardware—that means no middle man.
* **Para Virtualization**: Guest OS knows it is a virtual world and behaves as such, which is better for performance.
* **Hosted (Type 2):** Here hypervisor is on top of the pre-existing OS—some guest which never really goes.
* **OS Virtualization (Containers):** Multiple user spaces on the same system, literally an apartment to share with your roommates but you'd never see them.

Desktop, Server, Application and Storage Virtualization: lets you leverage virtualization at layer and component level ranging from desktops to storage to entire networks.

* **Real-World Use Case**

pretend for a moment that you own a company; want to save dollars? Studio run-away from your clunky, server room and jump on the data center express. Now you can create new virtual servers in minutes, typically instead of weeks for projects. More phablet, **VMware** (the Bey of virtualization) for instance will help businesses to consolidate servers and save a lot of money **In 2013 87% of organizations plan to virtualize their** **server** clear it far more popular than FREE pizza in the office

* **Performance and Security**

Super Powers with virtualization such as dynamic load balancing (no more server meltdown!), faster downtime, and seamless migration. That hardware utilization soars, you can scale faster (up or down) with no less yelling “cloud!” and it saves you space, power, and tension.

Wait but there is a but The dark side of virtualization. Attacks brought on by hypervisors:

**VM Escape:** a program in a virtual machine could escape the virtual machine and take over the host. Like teaching your goldfish how to drive.

**Inject malicious code**: If it gets through, the hackers are now going to place unspeakable shenanigans in your VMs.

**Exploiting hypervisor (the master of all VMS):** Oh buster, if the hypervisor is hacked, everyone dies.

**VM sprawl** : creating so many VMs that the data center turns into a digital jungle

**Side-Channel Attacks:** Lazy attackers can listen to resource use, and basically read secrets.

**VM Hack: Rootkit**:The VMs can be tampered with or infected by some of the sneak malware making it unfit to be trusted.

**Introduction :**

Virtualization is a key component in cloud computing, allowing multiple virtual machines (VMs) to run on a single physical server. This improves scalability, resource usage, and cost-efficiency for businesses and service providers. Virtualization is powered by hypervisors, which come in two main types: Type-1 (bare metal) and Type-2 (hosted). Popular tools like VMware, KVM, Xen, and Hyper-V are widely used. Despite its advantages, virtualization also presents major security challenges. Issues like VM escape, hyperjacking, side-channel attacks, and VM sprawl threaten system integrity. A single compromised VM could allow attackers to access the host or neighboring VMs. Real-world incidents, such as Spectre and Meltdown, have exposed the seriousness of these threats. This paper reviews the key vulnerabilities, technologies, real-world examples, and performance-security trade-offs associated with virtualization. It also provides a comparative analysis of selected academic sources to better understand these challenges and possible solutions【1】【2】【3】【4】.

**Literature Review** :

virtualization enables running several VMs on one physical machine but highlights serious threats like VM escape and hyperjacking. These attacks allow malware inside a VM to escape its boundaries and control the host or other VMs. The paper also mentions that tools like OpenStack can be used for scalable infrastructure, but a misconfigured firewall or hypervisor vulnerability can put all VMs at risk【1】.

focuses on cloud service providers. It states that 50% of users worry about provider security, and 52% of cloud attacks target web apps. Risks include unauthorized access by rogue administrators and data exposure between VMs due to poor isolation. It also highlights common performance problems when one VM uses excessive resources, affecting others on the same server【2】.

presents famous real-world examples such as CVE-2008-0923 (a shared folder flaw in VMware) and CPU-based Spectre/Meltdown attacks (CVE-2017-5753, CVE-2017-5718). These show how VMs can read host or neighbor data. The paper emphasizes the challenge of fixing such flaws without sacrificing performance【3】.

offers a detailed overview of virtualization types, such as full virtualization and OS-level containers. It outlines both benefits (like load balancing, resource sharing) and threats (like rootkits, VM sprawl, hypervisor exploits). The paper warns that a hacked hypervisor gives attackers total control over all hosted VMs【4】.

**Comparative Analysis :**

All four papers agree that virtualization is vital for modern IT but comes with serious security risks [1][3]both emphasize vulnerabilities like VM escape and side-channel attacks, showing how attackers can cross VM boundaries and compromise entire systems [2] [4] focus more on the risks from cloud providers, such as mismanagement, human error, or internal threats.

From a technical viewdiscuss hypervisors in detail, explaining how Type-1 hypervisors offer better security due to their direct interaction with hardware, while Type-2 hypervisors may be more vulnerable because they run on top of an operating system[1][3]

Performance trade-offs are a shared concern [3] illustrates how fixes for CPU vulnerabilities like Spectre/Meltdown reduce system performance [2] mentions VM performance issues when resources are poorly allocated.

In terms of solutions[4]

suggests careful VM management and monitoring, while recommends hardening hypervisors and regularly updating virtual images[1]

Overall, the papers collectively highlight that while virtualization is efficient, its risks require proactive management, updated security practices, and strong system configurations【1】【2】【3】【4】.

Security and Performance Implications :

Virtualization improves server efficiency, reduces costs, and increases flexibility. However, it also introduces major security risks like VM escape, hyperjacking, and side-channel attacks. These attacks allow hackers to steal data or control the hypervisor itself. Performance is affected when resources are not managed well or when security patches (e.g., for Spectre/Meltdown) slow down operations. VM sprawl and outdated VM images further expand the attack surface. Proper monitoring, isolation, and secure configuration are essential to maintaining a balance between performance and security in virtualized environments【1】【2】【3】【4】.

* ***Conclusion :***

This study highlights that virtualization is both powerful and risky. It enables better resource use and scalability but opens doors to complex attacks【1]. Key lessons include the importance of securing the hypervisor, managing VM images, and applying security patches promptly[2] Real-world examples like Spectre and CVE-2008-0923 show how devastating a single vulnerability can be [4] Organizations must prioritize isolation, monitoring, and staff training to mitigate these risks. With careful management, virtualization can remain a safe and efficient tool in IT and cloud environments [3】.