1. Threat Analysis of Cloud Services (Initial Thoughts for Discussion)

1.1 Hypervisor-based Threats

**Hypervisor-Threat 1:** Starvation of Resources & Denial of Service for some VMs:
Some VMs hog most of the processing and memory resources of the hypervisor host resulting in starvation of resources or complete denial of services for other VMs.

Probable Causes:
(a) Badly configured Resource Limits for some VMs
(b) A Rogue VM having the capability to bypass resource limits set in the Hypervisor

**Hypervisor-Threat 2:** VM Side-channel Attacks:
Malicious attack on one or more VMs residing in the same hypervisor host by a rogue VM.

Probable Causes:
(a) Lack of proper isolation of inter-VM traffic due to misconfiguration of the virtual network residing in the hypervisor.
(b) Limitation of packet inspection devices to handle high speed traffic (e.g., video traffic)
(c) Presence of VM Instances built from insecure VM Images (e.g., VM image having a Guest O/S without latest patches)

**Hypervisor-Threat 3:** Buffer overflow Attacks:
Buffer overflow Attacks

1.2 VM-based Threats

**VM-Threat 1:** Deployment of Rogue or Insecure VMs
Unauthorized users may create insecure instances from Images or may perform unauthorized administrative actions on existing VMs

Probable Causes:
(a) Improper configuration of access controls on VM administrative tasks such as Instance Creation, launching, suspension, re-activation etc.

**VM-Threat 2:** Presence of Insecure and Tampered Images
Due to lack of controls, the VM Image repository may contain insecure and tampered images.

Probable Causes:
(a) Lack of access control on who can put images into a repository
(b) Lack of mechanisms to verify the integrity of the images (e.g., digitally signed Image)