**1: What is the benefit of using a virtual machine in the following scenarios:**

**(a)** An operating system developer for MegaSoft, who is testing out a new kernel feature for the Doors operating system.

**Answer**: The benefit of using the virtual machine for the above scenario is that this will virtual machine give isolated environment for the testing and experimenting new kernel features. It the new features crashes or failed it will only be limited to the virtual machine not to the developer’s personal environment. It can be also deployed easily on many different hardware and software, which means it is portable too. Virtual machines also provide safe environment for the testing of new experiments which can cause damage and crash to the environment. So, by using the virtual machine if there was any crash or damage it won’t affect the developer environment or PC but will just damage the VM environment. So, you can just discard the previous crashed environment and start the new one.

**(b)** An employee of Bolton Anti-virus, who has received a new malware sample, and needs to figure out what the malware does.

**Answer**: The main benefit of using virtual machine for the testing of new malware sample is that if there was any vulnerability and security loophole it won’t damage the employee personal environment, but it will be just limited to the virtual machine environment, which won’t be that much problem if it crashed. Malware can also steal the sensitive data or do changes in the sensitive data on the host environment. By using VM it won’t be happened. One big advantage of using VM is that you can do the analysis of the malware behaviors very deeply, the forensic analysis. You can just check the behavior, the logs, the network traffic, the communication styles or patterns all by the VM.

**2: ChatTPG is an AI-based company that lets customers get answers from an AI chatbot. It runs its service from a large data center containing many servers. To serve customers using its software, ChatTPG is considering two options:**

(**a)** Install the ChatTPG software on each of the servers. Customers will log into the servers directly and interact with the chatbot.

**Answer**: By using the chatTPG software on each server this will just be inefficient and costly because the users won’t be utilizing the entire resource which is available for the use. One more difficulty in this model would be that if you were trying to increase the number of servers due to the increase of customers or any reason then it would be difficult in increasing the amount of software on every new server which is installed. It would be time consuming and would require complex work force too.

There can be also security weakness if the customers are directly logged in into the servers, they can do anything. We also need to prevent the servers from any unauthorized access from outside.

**(b)** Run hypervisors on the servers, with multiple virtual machines running on each hypervisor. The virtual machines will be equipped with the ChatTPG software. Customers will log into the virtual machines and interact with the chatbot there.

**Answer**: Having hypervisors on the servers would be good idea because it will have good utilization of the resources. The hypervisor will dynamically allocate the resource among the customers based on the requirements which will result in good server utilization. It will be also cost efficient. If the demand of resources has increase so increasing the VMs won’t be that big problem at that moment. We can just add the VMs to the existing clusters of the hypervisors and that will be easy to connect with host.

There will be also no security concerns because the customers will be connected to the hypervisors not directly to the software’s. Which won’t be any bread too because the customers won’t be directly communicating with the software. The security measure will be also centralized because of the hypervisors, which will be also easy to handle and manage it.

Which option would be better? Why? Please explain your choice with detailed justifications.

**Answer:** part no b is good, explain above.

**4: We discussed different types of hypervisors in module 3. If you are designing a cloud computing data center, which of these hypervisors would you choose? Please justify your choice of hypervisors.**

Answer: if I was designing a cloud computing data center, I would choose the type 1 hypervisor because of the performance, it is directly connected to the software of host computer, which will also help in utilizing the resources.

In this type of the security is also tight because of the isolation of host computer and virtual machines. The hypervisors run directly on the host computers that’s why it is trusted.

The ecosystem of the type 1 hypervisor is also accepted by most of the vendors in the market which is also a plus point.

In general, best security, performance, scalability and reliability were the reasons for which I will try to use the type 1 hypervisors.