**Virtualization and Cloud Security**

**Assignment-1**

**Q1. Explain the cloud delivery models.**

Ans: There are three types of Cloud service delivery models: Infrastructure as a Service (IAAS), Platform as a Service (PAAS), and Software as a Service (SAAS).

SaaS : Software as a Service (SaaS) is provided over the internet and requires no prior installation. These services can be availed from any part of the world at a minimal per month fee.

* Anywhere Accessibility – With SaaS, you can access the services from anywhere using any device such as smartphones, which eliminates the constraints set by on premise software.
* Affordable – SaaS is affordable as it eliminates the costs involved in the purchase, installation, maintenance and upgrades of computing hardware
* Ready to Use – You can quickly set up SaaS services so that they become functional in no time. All it takes is that you sign up for the service to get access to fast and powerful computing resources.

IaaS : The Infrastructure As A Service (IAAS) means the outsourcing of the physical infrastructure of IT (network, storage, and servers) from a third party provider. The IT resources are hosted on external servers and users can access them via an internet connection.

* Minimize Costs – Deploying an IaaS cloud model eliminates the need to deploy on premise hardware that reduces the costs.
* Enhanced Scalability – As the most flexible cloud computing model, IaaS allows you to scale the computing resources up or down based on demand.
* Simple Deployment – IaaS lets you easily deploy the servers, processing, storage, and networking to make it up and running in no time.

PaaS: Platform as a Service (PAAS) allows outsourcing of hardware infrastructure as well software environment, which includes databases, integration layers, runtimes and more.

* Minimal Development Time – PaaS reduces the development time since the vendor provides all computing resources like server-side components, which simplifies the process and improve the focus of the development team.
* Multiple Programming Language Support – PaaS offers support for multiple programming languages, which a software development company can utilize to build applications for different projects.
* Enhanced Collaboration – With PaaS, your business can benefit from having enhanced collaboration, which will help integrate your team dispersed across various locations.

**Q2. Briefly summarize the Types of Virtualization.**

Ans: Listed below are the types of Virtualization.

* Server virtualization: In server virtualization, one server appears as many. Each of these virtual servers may run the same or different operating systems. Server virtualization allows for lower power consumption, greater CPU utilisation and support for multiple operating systems.
* Desktop virtualization: This type of virtualization allows a user to switch between different operating systems on the same computer - it provides support for multiple operating systems and is therefore very convenient for developers and testers. This makes computer maintenance easy and reduces desktop IT staff administration. Using certain desktop virtualization techniques, an operating system environment can be provided on demand. Operating systems that reside within a virtualised environment are known as a guest operating systems.
* Virtual networks: A virtual network creates an illusion that a user is connected directly to a company network and resources, even though no such physical connection exists. Virtual networks are also known as VPNs or virtual private networks. Users can connect to a network and access the network resources from any computer that is connected to the Internet, using a virtual private network. Moreover, virtual networks allow network administrators to segment a network so that various departments (such as development, sales and management) appear to have their own separate networks.
* Virtual storage: Virtual storage allows applications and users with access to redundant and scalable physical storage, by using abstract (logical) file systems or a database interface.

**Q3. Write a short note on Host/Platform Security**

Ans: Host/platform security attempts to secure a resource by placing protection near it or adjusting and maintaining the resources so that it is not vulnerable to attacks. Two major approaches to host security are bastion host and OS hardening. A bastion host is a special purpose computer which is deliberately exposed on a public network and is designed to screen the rest of the network from security exposure. The other method is called OS hardening. An operating system needs to be hardened so that they are difficult to compromise. Hardening of an OS is the act of configuring an OS properly, updating it, creating policies to help control the system in a secure manner and removing unwanted applications and services. In order to increase the security of the host OS, the number of applications running on the host OS other than the hypervisor should be minimised. Applications that are not required should be removed. Other applications should be restricted to prevent malware from being installed on the system.

**Q4. Write down the points involved in Security recommendations for a guest OS**

Ans: Listed below are the points involved in Security recommendations for a guest OS

* Promptly install all updates to the guest OS. Operating systems have features that may automatically check for updates and install them.
* Recommended practices for managing the OS such as log management, time synchronisation, remote access, authentication etc. should be followed.
* Maintaining back up for a virtual drive used by a guest OS is needed on a regular basis.
* Disconnect the unused virtual hardware in each guest OS. This is important for virtual drives, virtual network adapters and serial and parallel ports.
* Separate authentication solutions are necessary for each guest OS unless there is a specific reason for two guest operating systems to share credentials.
* Make sure that virtual devices for the guest OS are associated only with the appropriate physical devices on the host system.

**Q5. Write down the points involved in Security recommendations for secure communications.**

Ans: Listed below are the security recommendations to secure communications:

* Guest OS should not have management network access; they may have network access to storage if necessary.
* Guest OS should be protected by a firewall running on the host OS or running locally. Firewall needs to filter malicious traffic using networking communications.
* Security of activities occurring between guest operating systems must be monitored. This is necessary because in a non-virtualised environment, communication is carried over networks and monitored by network security controls.
* If two guest operating systems are not communicating each other, then each should run on a separate virtual local area network.

**Q6. Explain security threats resulting from strong virtualization properties**

Ans: Listed below are the security threats resulting from strong virtualization properties:

* Untrusted components and the hypervisor trust model: The OS trusts the hardware in a physical system. Similarly, the OS trusts the virtual hardware and the hypervisor in a virtual machine. Therefore, secure virtualization bases its trust on the authenticity and integrity of a hypervisor.
* Transparent virtualization: A combination of the basic trust model with transparent virtualization denotes that a hypervisor is undetectable and is automatically trusted. Since a hypervisor has full control over system resources, it can alter any data inside the virtual machine and can create potential problems.
* Hypervisor insertion: There are various methods that are used to insert a hypervisor in operating system and to move the operating system from a physical to a virtual form. These hypervisor rootkits may create serious security risks as they may be used to alter an operating system completely. Since hypervisor is version specific and is less common in occurrences. These threats are with regard to hardware consideration of virtual components.
* Introspection and intervention by hypervisor: Introspection and intervention of the virtual machine by the hypervisor is a result of the ability of a hypervisor to take control of resources. A hypervisor can also observe Input/output channels to, from and within the virtual machine.
* Virtual machine scaling and cloning: Cloning of virtual machines can cause security concerns due to scaling, data retention, and management and identity issues. When the number of virtual machines increase, it will be difficult to manage these virtual machines. A clone of a virtual machine is identical to the original and thus can cause name and address collisions on a network.
* Monotonicity issues due to nonlinear virtual machine operations: The lack of linearity can create issues for data on the virtual machine, configuration and general logging and monitoring.
* Software decoupling from physical and hardware environment: Threats may occur due to the abstraction of virtual machine from hardware. These issues include being unable to locate the physical location of a virtual machine and thus creating problems in management and administration.