## PART-A

1) Define access control.

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.

2) List two states of cloud computing data.

Data at rest, Data in motion.

3) Define replay attack.

A replay attack is a form of network attack in which valid data transmission is maliciously or fraudulently repeated or delayed. The client receives the message twice.

4) Define security policy in cloud computing.

A cloud security policy is a formal guideline under which a company operates in the cloud. These instructions define the security strategy and guide all decisions concerning the safety of cloud assets.

5) List any two VM threat levels.

Low, medium, server.

Ex: Malware & Ransomware Attacks, Network Configuration.

## PART-B

6) a) List and explain the threats related to Data and Infrastructure.

### Threats related to Data

1. Logon Abuse

Logon abuse can refer to legitimate users accessing services of a higher security level that would normally be restricted to them. Unlike network intrusion, this type of abuse focuses primarily on those users who might be legitimate users of a different system or users who have a lower security classification.

2. Inappropriate System Use

This style of network abuse refers to the non-business or personal use of a network by otherwise authorized users, such as Internet surfing to inappropriate content sites (travel, pornography, sports, and so forth). As per the International Information Systems Security Certification Consortium (ISC) Code of Ethics and the Internet Advisory Board (IAB) recommendations, the use of networked services for other than business purposes can be considered abuse of the system. While most employers do not enforce extremely strict Web surfing rules, occasional harassment litigation may result from employees accessing pornography sites and employees operating private Web businesses using the company's infrastructure.

3. Eavesdropping

This type of network attack consists of the unauthorized interception of network traffic. Certain network transmission methods, such as satellite, wireless, mobile, PDA, and so on, are vulnerable to eavesdropping attacks. Tapping refers to the physical interception of a transmission medium (like the splicing of a cable or the creation of an induction loop to pick up electromagnetic emanations from copper). Eavesdropping can take one of two forms: Passive eavesdropping and Active eavesdropping.

4. Network Intrusion

This type of attack refers to the use of unauthorized access to break into a network primarily from an external source. Unlike a logon abuse attack, the intruders are not considered to be known to the company. Most common hacks belong to this category. Also known as a penetration attack, it exploits known security vulnerabilities in the security perimeter.

## Data and Cloud Access Control Issues

The cost of access control in the cloud must be commensurate with the value of the information being protected. The value of this information is determined through qualitative and quantitative methods. These methods incorporate factors such as the cost to develop or acquire the information, the importance of the information to an organization and its competitors, and the effect on the organization's reputation if the information is compromised. Proper access controls enable full availability. Availability ensures that a system's authorized users have timely and uninterrupted access to the information in the system. Access control must offer protection from an unauthorized, unanticipated, or unintentional modification of information. This protection should preserve the data's internal and external consistency. The confidentiality of the information must also be similarly maintained, and the information should be available on a timely basis. The following measures compensate for both internal and external access violations:

1. Backups
2. RAID (Redundant Array of Independent Disks) technology
3. Fault tolerance
4. Business continuity planning
5. Insurance

7) a) Explain the CIA triad in cloud computing.

### The CIA Triad

Confidentiality, integrity, and availability are sometimes known as the CIA triad of information system security, and are important pillars of cloud software assurance.

### Confidentiality

Confidentiality refers to the prevention of intentional or unintentional unauthorized disclosure of information. Confidentiality in cloud systems is related to the areas of intellectual property rights, covert channels, traffic analysis, encryption, and inference:

Intellectual property rights: Intellectual property (IP) includes inventions, designs, and artistic, musical, and literary works. Rights to intellectual property are covered by copyright laws, which protect creations of the mind, and patents, which are granted for new inventions.

Covert channels: A covert channel is an unauthorized and unintended communication path that enables the exchange of information. Covert channels can be accomplished through timing of messages or inappropriate use of storage mechanisms.

Traffic analysis: Traffic analysis is a form of confidentiality breach that can be accomplished by analyzing the volume, rate, source, and destination of message traffic, even if it is encrypted. Increased message activity and high bursts of traffic can indicate a major event is occurring. Countermeasures to traffic analysis include maintaining a near-constant rate of message traffic and disguising the source and destination locations of the traffic.

Encryption: Encryption involves scrambling messages so that they cannot be read by an unauthorized entity, even if they are intercepted. The amount of effort (work factor) required to decrypt the message is a function of the strength of the encryption key and the robustness and quality of the encryption algorithm.

Inference: Inference is usually associated with database security. Inference is the ability of an entity to use and correlate information protected at one level of security to uncover information that is protected at a higher security level.

**Integrity**

The concept of cloud information integrity requires that the following three principles are met:

1. Modifications are not made to data by unauthorized personnel or processes.
2. Unauthorized modifications are not made to data by authorized personnel or processes.
3. The data is internally and externally consistent — in other words, the internal information is consistent both among all sub-entities and with the real-world, external situation.

**Availability**

Availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. Availability guarantees that the systems are functioning properly when needed. In addition, this concept guarantees that the security services of the cloud system are in working order. A denial-of-service attack is an example of a threat against availability. The reverse of confidentiality, integrity, and availability is disclosure, alteration, and destruction (DAD).

b) Outline the risks that involved with the Cloud service provider.

**1. Limited Visibility into Network Operations** When shifting your data from one source to another, you also transfer the responsibility of managing a part of it from your in-house team to the CSP (cloud service provider). Unless you know what, you are doing, it can lead to a loss of visibility into your resources, leading to an increase in service usage and costs.

**2. Malware** About 90% of organizations moving to the cloud are more likely to experience data breaches. Cloud computing partners have tried to build in all the major security protocols to keep your data safe. They have familiarised themselves with these modern technologies. As a result, they are now capable of bypassing most of these standards and accessing sensitive user information with ease.

**3. Compliance** Cloud computing is scaling at a trailblazing speed. While it has helped organizations shift from offline systems faster, it has also raised the necessary questions on compliance. So, you must ensure that data access and storage need across your PII (Personally Identifiable Information) are matched by the cloud computing provider with the requisite privacy and security rules.

**4. Data loss** With brands shifting a part of their control to the CSP, they also allow their data to be more vulnerable. For example, if there is a data breach in the cloud computing provider's space, the chances of your enterprise's sensitive data landing in the wrong hands increase manifold.

**5. Inadequate Due Diligence**

Due diligence helps understand the efforts an enterprise needs to put in to transfer its data to the cloud. Often, we come across companies that overlook or are not stringent enough in understanding how much work is necessary for

- a smooth transition process, and
- steps taken by the cloud computing provider to ensure the same

8) a) Explain the concept of virtualization security management.

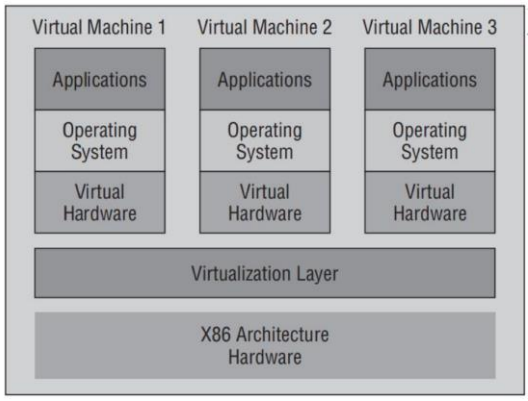
Virtualization Security Management: Although the global adoption of virtualization is a relatively recent event, threats to the virtualized infrastructure are evolving just as quickly. Historically, the development and implementation of new technology has preceded the full understanding of its inherent security risks, and virtualized systems are no different. The following sections examine the threats and vulnerabilities inherent in virtualized systems and look at some common management solutions to those threats. VIRTUALIZATION TYPES The Virtual Machine (VM), Virtual Memory Manager (VMM), and hypervisor or host OS are the minimum set of components needed in a virtual environment. They comprise virtual environments in a few distinct ways:

1. Type 1 virtual environments are considered "full virtualization" environments and have VMs running on a hypervisor that interacts with the hardware.
2. Type 2 virtual environments are also considered "full virtualization" but work with a host OS instead of a hypervisor.
3. Para-virtualized environments offer performance gains by eliminating some of the emulation that occurs in full virtualization environments.
4. Other type designations include hybrid virtual machines (HVMs) and hardware-assisted techniques.

VIRTUALIZATION MANAGEMENT ROLES

Typically, the VMware Infrastructure is managed by several users performing different roles. The roles assumed by administrators are the Virtualization Server Administrator, Virtual Machine Administrator, and Guest Administrator. VMware Infrastructure users may have different roles and responsibilities, but some functional overlap may occur. The roles assumed by administrators are configured in VMS and are defined to provide role responsibilities:

1. Virtual Server Administrator — This role is responsible for installing and configuring the ESX Server hardware, storage, physical and virtual networks, service console, and management applications.
2. Virtual Machine Administrator — This role is responsible for creating and configuring virtual machines, virtual networks, virtual machine resources, and security policies. The Virtual Machine Administrator creates, maintains, and provisions virtual machines.
3. Guest Administrator — This role is responsible for managing a guest virtual machine or machines. Tasks typically performed by Guest Administrators include connecting virtual devices, adding system updates, and managing applications that may reside on the operating system.




9) a) Explain the security requirements for cloud architecture.

One goal for architecture is that it should be appropriate in meeting needs. This section surveys key architectural requirements for a typical cloud implementation. Several factors serve as the underlying motivation for requirements; these include:

1. Costs and Resources The cloud provider's financial resources will act to constrain investment in technology, security controls included. But it is important to recognize that the absence of unlimited resources can be very motivating to how one designs, architects, and builds. For instance, if you know that your staff will be small, then this can force you toward process improvement and greater automation. Likewise, cost is also a motivation for the consumer of cloud services. The nature of these constraints tends toward the development of services with operating characteristics that are not ideal for all consumers
2. Reliability This is a quality that refers to the degree you can depend on a system to deliver its stated services. Reliability can be described as a guarantee that the underlying technology can provide delivery of services.
3. Performance A measure of one or more qualities that have to do with the usefulness of a system. By example, common measures include responsiveness to input and the amount of throughput the system can handle.
4. The Security Triad The essential security principles of confidentiality, integrity, and availability apply to most systems; the responsibility of a security architect is to match security controls with security requirements that sometimes must be derived from the need to assure the other three drivers (reliability, performance, and cost).
5. Legal and regulatory constraints Legal and regulatory constraints can lead to the need for many additional requirements having to do with technical security controls, access policies, and retention of data among many others.

10) a) Explain the best practices towards cloud security.

The Cloud Computing Use Case Discussion Group is focused on best practices for building clouds or IaaS and PaaS. In July 2010, they published version 4.0 of their Cloud Computing Use Cases White Paper. Besides detailing several use cases for cloud computing, this group also identified several security controls for cloud computing. The following summarizes these

• Asset Management All assets including hardware, network, and software that comprise the cloud infrastructure must be managed.

• Cryptography: Key and Certificate Management They advocate for an infrastructure to manage keys and certificates, and encourage the use of standards-based cryptography.

• Data/Storage Security: They identify the need to support encrypted storage of data and they recognize that some users will need separate storage from others.

• Endpoint Security: Secure endpoints for cloud resources, along with end point restrictions by protocol and device types.

• Event Auditing and Reporting: This entails visibility by consumers into security-relevant events and breaches.

• Identity, Roles, Access Control, and Attributes: Effective implementation of access controls and security policy enforcement depends on defined identity, roles, and privileges.

• Network Security Network traffic must be able to be secured at the level of switches, routers, and packets.

• Other controls listed by the Cloud Computing Use Case Discussion Group Service Automation, Workload and Service Management, and Security Practices.

11) a) Explain about Data encryption related to cloud environment with advantages and challenges.

Cryptography is a complex and esoteric field. In modern times, cryptography has expanded from protecting the confidentiality of private communications to including techniques for assuring content integrity, identity authentication, and digital signatures along with a range of secure computing techniques. Given that range of functional utility, cryptography has been recognized as being a critical enabling technology for security in cloud computing. Focusing on data security, cryptography has great value for cloud computing.

This use of public–private keys is a great enabler for confidentiality in cloud computing, and not just for encryption of content. A private key can be used to authenticate a user or computational component, and it can also be used to initiate the negotiation of a secure channel or connection between communicating parties. Going one level deeper in our background treatment of cryptography, for the purpose of this book, there are four basic uses of cryptography:

• Block Ciphers: These take as input a key along with a block of plaintext and output a block of cyphertext. Because messages are generally larger than a defined block, this method requires some method to associate or knit together successive cyphertext blocks.

• Stream Ciphers: These operate against an arbitrarily long stream of input data, which is converted to an equivalent output stream of cyphertext.

• Cryptographic Hash Functions: Hash functions take an arbitrarily long input message and output a short, fixed length hash. A hash can serve various purposes, including as a digital signature or to verify the integrity of the message.

• Authentication Cryptography: is also widely used within authentication and identity management systems.

**Advantages**

1. Encryption Provides Privacy − Data Encryption is not only beneficial for organization or the military, but normal computer users can also use it to save sensitive data including Bank Account details, medical records, etc., safe. Without proper Encryption, anyone who can access the device will be capable to view and copy it.
2. Always Providing Security − There are several tools to password protect a folder or some local storage information that someone it can choose, but it is the only true way to secure information in its entirety. This is possible because without proper decryption of information, no one can use it.
3. Protects data in cloud storage − When data is saved in the public cloud, it can be exposed to a much broader range of threats, such as accidental exposure to the Internet, access by some cloud tenants, and by malicious insiders at the cloud provider. Encrypting information in cloud storage by default supported a layer of security against all these threats.
4. Protects intellectual property − Intellectual property is a strategic asset that can be value millions. By encrypting this information and securely handling encryption keys, an organization can render it counterproductive to an attacker.

**Challenges**

1. Managing encryption keys requires more overhead - Managing encryption keys is arguably the most challenging part of implementing an encryption strategy.
2. Difficulty in accessing the encrypted data - Investing in technology that comes with its own proprietary components and adoption barriers can present more encryption issues, so it is smarter to utilize a key management system that can integrate with the existing technology already deployed in your network.
3. Difficulty integrating with cloud-based systems - Integrating a Key Management System with cloud products introduces an entire new set of problems, as there are difficulties within the IaaS, PaaS, and SaaS models of cloud computing. To keep it simple, the root of the complexities lies in the different infrastructures and the Cloud providers.