CC MOD 4 NOTES

4.1

Security Issues in Cloud Computing :

1. **Data Loss –**
   Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of Somebody else, and we don't have full control over our database. So, if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.
2. **Interference of Hackers and Insecure API's –**
   We know that the easiest way to communicate with Cloud is using API. So it is important to protect the Interface's and API's which are used by an external user. But also in cloud computing, few services are available in the public domain which are the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So, it may be possible that with the help of these services hackers can easily hack or harm our data.
3. **User Account Hijacking –**
   Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by a hacker then the hacker has full authority to perform Unauthorized Activities.
4. **Changing Service Provider –**
   Vendor lock-In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they face various problems like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc.

5. **Denial of Service (DoS) attack –**
   This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs, data is lost. So, in order to recover data, it requires a great amount of money as well as time to handle it.

6. **Shared Resources:** Cloud computing relies on a shared infrastructure. If one customer's data or applications are compromised, it may potentially affect other customers sharing the same resources, leading to a breach of confidentiality or integrity.

7. **Insider Threats:** Employees or service providers with access to cloud systems may misuse their privileges, intentionally or unintentionally causing data breaches. Proper access controls and monitoring are essential to mitigate these threats.

8. **Social Engineering and Phishing:** Attackers may use social engineering tactics to trick users or cloud service providers into revealing sensitive information or granting unauthorized access.

9. **IoT Devices and Edge Computing:** The proliferation of IoT devices and edge computing can increase the attack surface. These devices often have limited security controls and can be targeted to gain access to cloud resources.

10. **Shadow IT:** People and departments within an enterprise often deploy new cloud apps and services without the approval, or even awareness, of IT security managers. These services may result in data loss, data oversharing, compliance issues, and more.

Information Security

1. The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability.
2. Here, integrity means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
3. Confidentiality means preserving authorized restrictions on disclosure and access, including means for defending proprietary and personal privacy information.
4. And availability means ensuring timely and reliable access to and use of information.
5. Cloud computing provides computing and storage resources on demand without the need for internal infrastructure which ensures cost-saving benefits. As the technology arrangement becomes more popular, additional cloud computing security measures are necessary to ensure the continued protection of the confidentiality, availability, and integrity of enterprise data.
6. The physical boundaries of data and moving that data between trusted partners securely and reliably is changed by cloud computing.
7. To ensure the latest security capabilities are being used properly, this capability of cloud computing will require encryption and trust models being constantly evaluated. By using the right service provider in the cloud, this capability may be enhanced. To ensure information security data storage and privacy security need to be consider.

Data Storage Security

For Data Storage Security Data storage zoning, Data tagging, Data retention policies, Data permanence/deletion, Data classification, Locality requirements, etc. have to be in the check list.

Data Privacy Security

Backup, Archiving, Multi-tenancy issues, Recovery, Privacy/privacy controls, prevention, Malicious data aggregation, Encryption (at-rest, in-transit, key management, Federal information processing standards/Federal

information security management act), Digital signing/integrity, attestation, Data leak prevention etc. are need to be considered for Data Privacy Security

Identity management and access control:

It is a combination of policies and technologies that allows organizations to identify users and provide the right form of access as and when required. IAM allows you to manage users and their level of access to the aws console. AWS Identity and Access Management is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. With IAM, Organizations can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access. IAM enables the organization to create multiple users, each with its own security credentials, controlled and billed to a single aws account. IAM allows the user to do only what they need to do as a part of the user's job.

Features of IAM

- **Centralised control of your AWS account:** You can control creation, rotation, and cancellation of each user's security credentials. You can also control what data in the aws system users can access and how they can access.
- **Granular permissions:** It is used to set a permission that user can use a particular service but not other services.
- **Identity Federation:** An Identity Federation means that we can use Facebook, Active Directory, LinkedIn, etc with IAM. Users can log in to the AWS Console with same username and password as we log in with the Active Directory, Facebook, etc.
- **Multifactor Authentication:** An AWS provides multifactor authentication as we need to enter the username, password, and security check code to log in to the AWS Management Console.
- **Permissions based on Organizational groups:** Users can be restricted to the AWS access based on their job duties, for example, admin, developer, etc.

- **Eventually Consistent:** IAM service is eventually consistent as it achieves high availability by replicating the data across multiple servers within the Amazon's data center around the world.
- **Free to use:** AWS IAM is a feature of AWS account which is offered at no additional charge. You will be charged only when you access other AWS services by using IAM user.

IAM Identities Classified As

1. IAM Users
2. IAM Groups
3. IAM Roles

Root user

- The root user will automatically be created and granted unrestricted rights. We can create an admin user with fewer powers to control the entire Amazon account.
- When you first create an AWS account, you create an account as a root user identity which is used to sign in to AWS.
- You can sign to the AWS Management Console by entering your email address and password. The combination of email address and password is known as **root user credentials**.
- The Root user can also access the billing information as well as can change the password also.

IAM Users

We can utilize IAM users to access the AWS Console and their administrative permissions differ from those of the Root user and if we can keep track of their login information.

Example

With the aid of IAM users, we can accomplish our goal of giving a specific person access to every service available in the Amazon dashboard with only a limited set of permissions, such as read-only access. Let's say user-

1 is a user that I want to have read-only access to the EC2 instance and no additional permissions, such as create, delete, or update. By creating an IAM user and attaching user-1 to that IAM user, we may allow the user access to the EC2 instance with the required permissions.

IAM Groups

A group is a collection of users, and a single person can be a member of several groups. With the aid of groups, we can manage permissions for many users quickly and efficiently.

Example

Consider two users named user-1 and user-2. If we want to grant user-1 specific permissions, such as the ability to delete, create, and update the auto-calling group only, and if we want to grant user-2 all the necessary permissions to maintain the auto-scaling group as well as the ability to maintain EC2,S3 we can create groups and add this user to them. If a new user is added, we can add that user to the required group with the necessary permissions.

IAM Roles

While policies cannot be directly given to any of the services accessible through the Amazon dashboard, IAM roles are similar to IAM users in that they may be assumed by anybody who requires them. By using roles, we can provide AWS Services access rights to other AWS Services.

Example

Consider Amazon EKS. In order to maintain an autoscaling group, AWS eks needs access to EC2 instances. Since we can't attach policies directly to the eks in this situation, we must build a role and then attach the necessary policies to that specific role and attach that particular role to EKS.

IAM Policies

IAM Policies can manage access for AWS by attaching them to the IAM Identities or resources IAM policies defines permissions of AWS identities and AWS resources when a user or any resource makes a request to AWS will validate these policies and confirms whether the request to be

allowed or to be denied. AWS policies are stored in the form of Jason format the number of policies to be attached to particular IAM identities depends upon no.of permissions required for one IAM identity. IAM identity can have multiple policies attached to them.

Use cases Identity and Access Management(IAM)

1. **Resource Access Control:** Identity and access management (IAM) will allows you to manage the permissions to the resources in the AWS cloud like users who can access particular serivce to which extent and also instead of mantaing the permissions individually you can manage the permissions to group of users at a time.
2. **Managing permissions:** For example you want to assign an permission to the user that he/her can only perform restart the instance task on AWS EC2 instance then you can do using AWS IAM.
3. **Implemneting role-based access control(RBAC):** Identity and Access Management(IAM) will helps you to manage the permissions based on roles Roles will helps to assign the the permissions to the resourcesw in the AWS like which resources can access the another resource according to the requirement.
4. **Enabling single sign-on (SSO):** Identity and Access Management will helps you to maintain the same password and user name which will reduce the effort of remembering the different password.

Design Principles

There are six design principles for security in the cloud:

- Implement a strong identity foundation:

  Implement the principle of least privilege and enforce separation of duties with the appropriate authorization for each interaction with your AWS resources. Centralize privilege management and reduce or even eliminate reliance on long-term credentials.

- ### Enable traceability:

  Monitor, alert, and audit actions and changes to your environment in real-time. Integrate logs and metrics with systems to automatically respond and take action.

- ### Apply security at all layers:

  Rather than just focusing on protecting a single outer layer, apply a defense-in-depth approach with other security controls. Apply to all layers, for example, edge network, virtual private cloud (VPC), subnet, load balancer, every instance, operating system, and application.

- ### Automate security best practices:

  Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost-effectively. Create secure architectures, including the implementation of controls that are defined and managed as code in version-controlled templates.

- ### Protect data in transit and at rest:

  Classify your data into sensitivity levels and use mechanisms, such as encryption and tokenization where appropriate. Reduce or eliminate direct human access to data to reduce the risk of loss or modification.

- ### Prepare for security events:

  Prepare for an incident by having an incident management process that aligns with your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

Cloud security management frameworks:

Cloud security management frameworks provide structured guidelines and best practices that organizations can follow to ensure their cloud environments are secure and compliant with industry standards. These frameworks offer a systematic approach to managing and mitigating risks associated with cloud computing. Here are some of the most prominent and widely adopted cloud security management frameworks:

Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

- **Overview**: The CSA CCM is a comprehensive framework of security controls specifically designed for cloud computing environments. It covers fundamental security principles across 16 domains, including compliance, data security, identity and access management, and infrastructure security.
- **Benefits**: Provides a detailed, standardized baseline of security best practices. The CCM is well-recognized in the industry and helps align security measures with compliance requirements.

2. NIST Cloud Computing Security Reference Architecture

- **Overview**: This framework from the National Institute of Standards and Technology (NIST) provides a detailed understanding of the security components that are necessary for cloud computing. It integrates NIST's broader cybersecurity frameworks and standards to address the specific needs of cloud security.
- **Benefits**: Offers a highly structured approach to security that can be applied across different types of cloud services (IaaS, PaaS, SaaS). It helps organizations ensure they are compliant with federal guidelines and standards.

3. ISO/IEC 27017

- **Overview**: An international standard specifically focused on cloud security, providing guidelines on the information security aspects of cloud computing, recommending controls and implementation guidance for both cloud service providers and cloud service customers.
- **Benefits**: Provides an internationally recognized framework that extends the ISO/IEC 27001 and 27002 standards for information security management to the specific mechanisms of cloud computing.

Implementing a Framework

When choosing and implementing a cloud security management framework, consider the following steps:

- **Assess Needs and Compliance Requirements**: Determine what specific security and compliance needs align with your industry and type of cloud deployment.
- **Choose a Suitable Framework**: Select a framework that best fits your organizational needs, regulatory requirements, and cloud architecture.
- **Implement Controls and Policies**: Adapt the framework’s guidelines into actionable policies and controls within your cloud environments.
- **Continuous Monitoring and Improvement**: Use tools and strategies to continuously monitor security posture and compliance, adapting to new threats and changes in the cloud landscape.

4.2

Host and data security in SaaS, PaaS, IaaS

Securing hosts and data across Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) requires a layered approach that addresses the unique security challenges and responsibilities associated with each service model.

SaaS and Paas Host Security

Generally, the cloud service providers do not share information regarding their host platforms, hosts OS, and the processes that are in place to secure the hosts, as hackers might exploit that information when they are trying to break into the cloud services. Hence, in the context of System as a service(SaaS) or Platform as a service(PaaS) cloud services security of the host should be non-transparent with the customers and the responsibility of securing the host is confined to the cloud service providers.

- Virtualization is a technique that improves the host's hardware utilization, along with other benefits, it is common for cloud service providers to employ virtualization platforms including VMware hypervisors and XEN, in their host's computing platform architecture. Apart from this one should be aware of how his provider is using the virtualization technology and the provider's process for securing the virtualization layer.
- Both the SaaS and PaaS delivery models software platforms should abstract the host operating system from the end user with a host abstraction layer. The accessibility of the abstraction layer is different in each one of the delivery models (SaaS and PaaS).
- In System as a Service, the abstraction layer is hidden from the users and only available to the developers and the cloud service provider's operational staff.
- Whereas in Platform as a Service users have indirect access to the abstraction layer in the form of PaaS API(Application

programming interface) that eventually interacts with the host abstraction layer.

- Thus, the customers of System as a Service(SaaS) and Platform as a Service(Paas) rely on the cloud service providers to provide a secure host platform on which the application is developed and deployed.

Data Security: FOR SAAS

1. **Data Encryption**: Data should be encrypted both at rest and in transit using strong encryption algorithms.
2. **Data Loss Prevention (DLP)**: Implement DLP solutions to monitor and control data transfers to and from the SaaS application to prevent unauthorized data leakage.
3. **Access Control**: Implement role-based access control (RBAC) to ensure that only authorized users can access specific data sets or perform certain actions within the SaaS application.

Data Security:FOR PAAS

1. **Database Security**: Use encrypted databases, secure database connections, and implement strong database access controls.
2. **API Security**: Secure APIs with authentication, authorization, and encryption to protect data exchanged between applications and services on the PaaS platform.
3. **Backup and Recovery**: Regularly back up data and ensure that backup processes are secure to prevent data loss and facilitate recovery in case of failures.

Infrastructure as a Service(IaaS)

Host Security

The customers of Infrastructure as a Service(IaaS) are primarily responsible for securing the hosts in the cloud, Infrastructure as a Service(IaaS) employs virtualization at the host layer, IaaS host security can be categorized as follows:

1. *Virtualization Software Security*

It provides customers to create and terminate virtual instances. Virtualization can be achieved by using virtualization models such as:-OS-level virtualization, paravirtualization, or hardware-based virtualization. In public, IaaS application customers do not have access to this software layer as it is managed by cloud service providers.

2. *Customer Guest OS or Virtual Server Security*

The virtual instance of an operating system is placed above the virtualization layer and is visible to customers from the internet. Customers have full access to virtual servers. For example:- various versions of Linux, Microsoft, and Solaris are available in amazon's aws for creating an instance.

3. *Virtual Server Security*

The customers of Infrastructure as a Service(IaaS) have full access to the virtualized guest virtual machines that are hosted and isolated from each other by hypervisor technology. Thus, customers are responsible for the security management of the guest virtual machines. A public Infrastructure as a Service(IaaS) offers a web service API to perform management functions such as provisioning, decommissioning, and duplication of virtual servers on the IaaS platform itself.

Host Security Threats in the Public IaaS

- Deployment of malware embedded in software components in the virtual machines.
- Attack on that system which is not properly secured by the host firewalls
- Attacks on accounts that are not properly secured eg. weak passwords, repetitive passwords, etc.
- Stealing keys that will be used to access and manage hosts(SSH private keys).

Data Security:

1. *Storage Encryption*: Encrypt data stored in cloud storage using encryption mechanisms provided by the IaaS provider or third-party solutions.

2. *Data Integrity*: Implement data integrity checks and monitoring to detect unauthorized changes to data stored in IaaS environments.

3. *Access Management*: Use IAM tools to control access to IaaS resources, implement strong authentication mechanisms, and enforce least privilege access principles.