Cloud Security and Compliance

Prepared By:

D.R.Gandhi

Lecturer in IT

DR. S & S.S. Ghandhy College Of Engg. & Tech.,Surat

Learning Outcome

- Security in the Cloud
  - Cloud security challenges
  - Identity and access management
  - Access control and authentication in cloud computing
- Data Security in Cloud
  - Technologies for Data security in Cloud
- Securing Private and Public Cloud Architecture
  - Metrics for Service Level Agreements(SLAs)
  - DevSecOps

Security in the Cloud

Cloud Security:-

- ***Cloud security is a collection of procedures and technology designed to address external and internal threats to business security.***
- Organizations need cloud security as they move toward their digital transformation strategy and incorporate cloud-based tools and services as part of their infrastructure.
- *Cloud security refers to the policies, controls, procedures, and technologies that protect cloud-based systems, data, and infrastructure from threats and vulnerabilities.*
- It is a critical aspect of cloud computing, as organizations are entrusting their sensitive data and applications to cloud service providers (CSPs).

Security in the Cloud

Cloud Security:-

- Cloud security is the set of control-based security measures and technology protection, designed to protect online stored resources from leakage, theft, and data loss.
- Protection includes data from cloud infrastructure, applications, and threats. Security applications uses a software the same as SaaS (Software as a Service) model.
- Security in the cloud refers to the measures, practices, and technologies employed to protect data, applications, and infrastructure hosted in cloud computing environments.
- Cloud security aims to address the unique security challenges that arise when organizations leverage cloud services and resources provided by third-party cloud service providers (CSPs).

Security in the Cloud

Advantages of Cloud Security:-

- *Data Security:-*Ensuring the confidentiality, integrity, and availability of data stored in the cloud is a primary concern. This includes data encryption (both at rest and in transit), access controls, and data backup and recovery mechanisms.
- *Identity and Access Management (IAM):* Robust authentication and authorization mechanisms are essential to control who can access cloud resources and with what privileges. IAM includes features like multi-factor authentication (MFA), role-based access controls (RBAC), and federated identity management.
- *Network Security:* Securing the network infrastructure that connects cloud resources and protects against threats like distributed denial-of-service (DDoS) attacks, man-in-the-middle (MITM) attacks, and unauthorized access attempts.

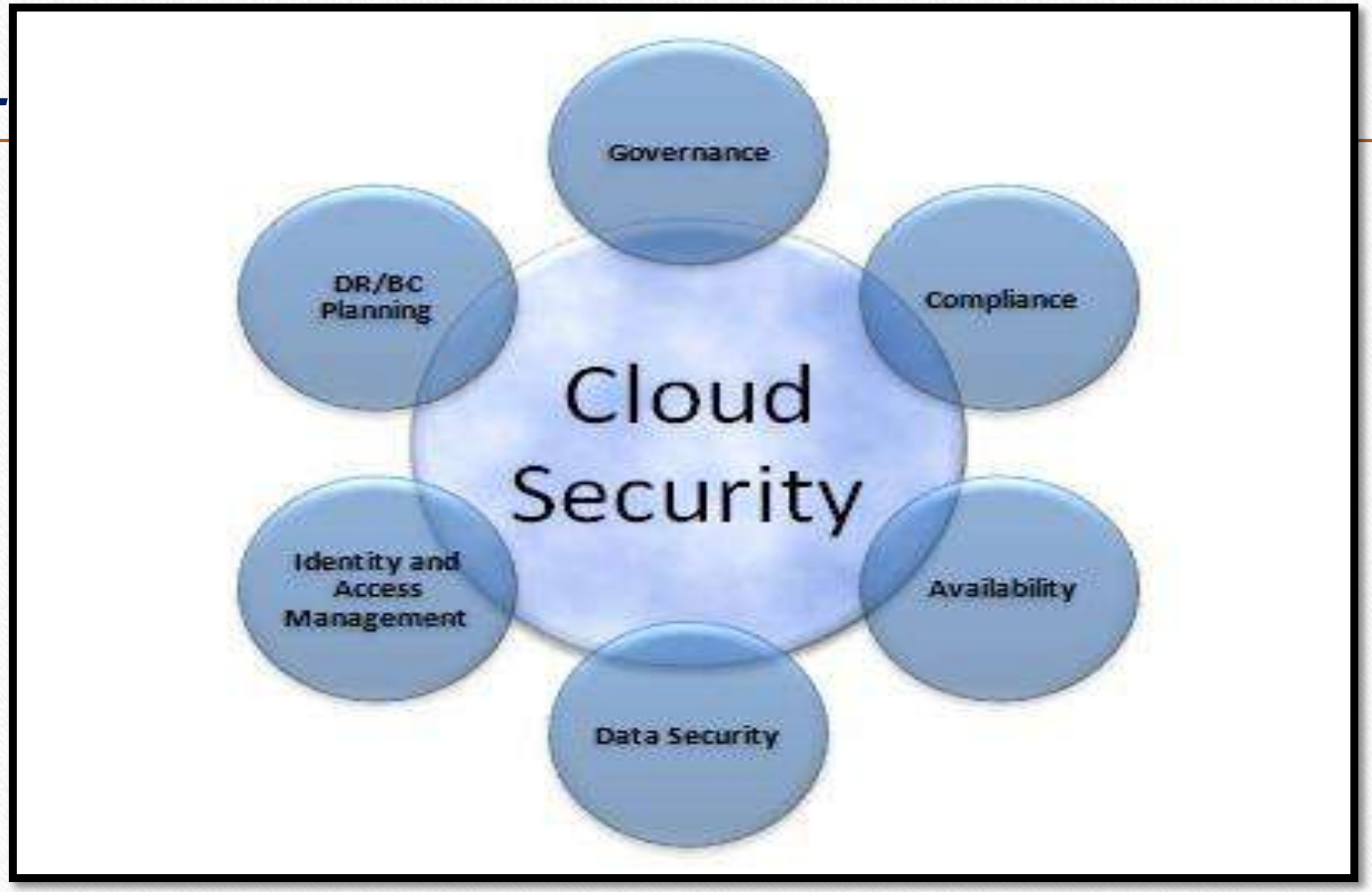
Security in the Cloud

Advantages of Cloud Security:-

- *Security Automation and DevSecOps:* Incorporating security practices into the software development lifecycle (DevSecOps) and leveraging automation tools to streamline security processes and improve overall security posture.
- *Shared Responsibility Model:* Cloud security is a shared responsibility between the cloud service provider (CSP) and the customer. The CSP is responsible for securing the underlying infrastructure, while the customer is responsible for securing their data, applications, and access controls.

Security in the Cloud

Cloud Security:-



Challenges of Cloud Security

- *Data security*
- *Identity and access management (IAM)*
- *Cloud misconfiguration*
- *Shared responsibility model*
- *Compliance and regulatory requirements*
- *Insider threats*
- *Vendor lock-in and migration challenges*
- *Distributed denial of service (DDoS) attacks*

Challenges of Cloud Security

Data security:-

- One of the primary concerns in cloud computing is data security.
- Organizations need to ensure that their data is protected from unauthorized access, theft, or loss while stored in the cloud.
- Data encryption, access controls, and data governance policies play a crucial role in maintaining data security in the cloud.

Challenges of Cloud Security

Identity and access management (IAM):-

- Proper identity and access management is essential for securing cloud resources.
- Organizations must implement robust authentication and authorization mechanisms to ensure that only authorized users and applications can access cloud resources.
- IAM also involves managing user permissions, roles, and access controls across multiple cloud services and environments.

Challenges of Cloud Security

Cloud misconfiguration :-

- Misconfigured cloud services can lead to security vulnerabilities and potential data breaches.
- Cloud providers offer a wide range of security configurations, and it is crucial for organizations to correctly configure these settings based on their specific security requirements and industry best practices.

Challenges of Cloud Security

Shared responsibility model :-

- In cloud computing, security responsibilities are shared between the cloud provider and the customer.
- Understanding and adhering to this shared responsibility model is essential to ensure that both parties fulfill their respective security obligations effectively.

Challenges of Cloud Security

Compliance and regulatory requirements:-

- Organizations operating in regulated industries, such as healthcare, finance, or government, must comply with various regulatory requirements and industry standards.
- Ensuring compliance with these regulations in the cloud environment can be challenging, as organizations need to maintain visibility and control over their data and workloads.

Challenges of Cloud Security

Insider threats :-

- Cloud computing environments are not immune to insider threats, which can arise from malicious or negligent actions by employees, contractors, or other authorized users.
- Organizations must implement effective monitoring, logging, and incident response measures to detect and mitigate insider threats.

Challenges of Cloud Security

Vendor lock-in and migration challenges:-

- Migrating data and applications between different cloud providers or from the cloud back to an on-premises environment can be complex and challenging.
- Organizations should carefully consider vendor lock-in risks and have a well-defined strategy for migrating or exiting cloud services if needed.

Challenges of Cloud Security

Distributed denial of service (DDoS) attacks :-

- Cloud-based services and applications can be targeted by DDoS attacks, which can overwhelm the resources and cause service disruptions.
- Organizations must implement effective DDoS mitigation strategies and work closely with cloud providers to protect against these attacks.

Identity and access management

IAM:-

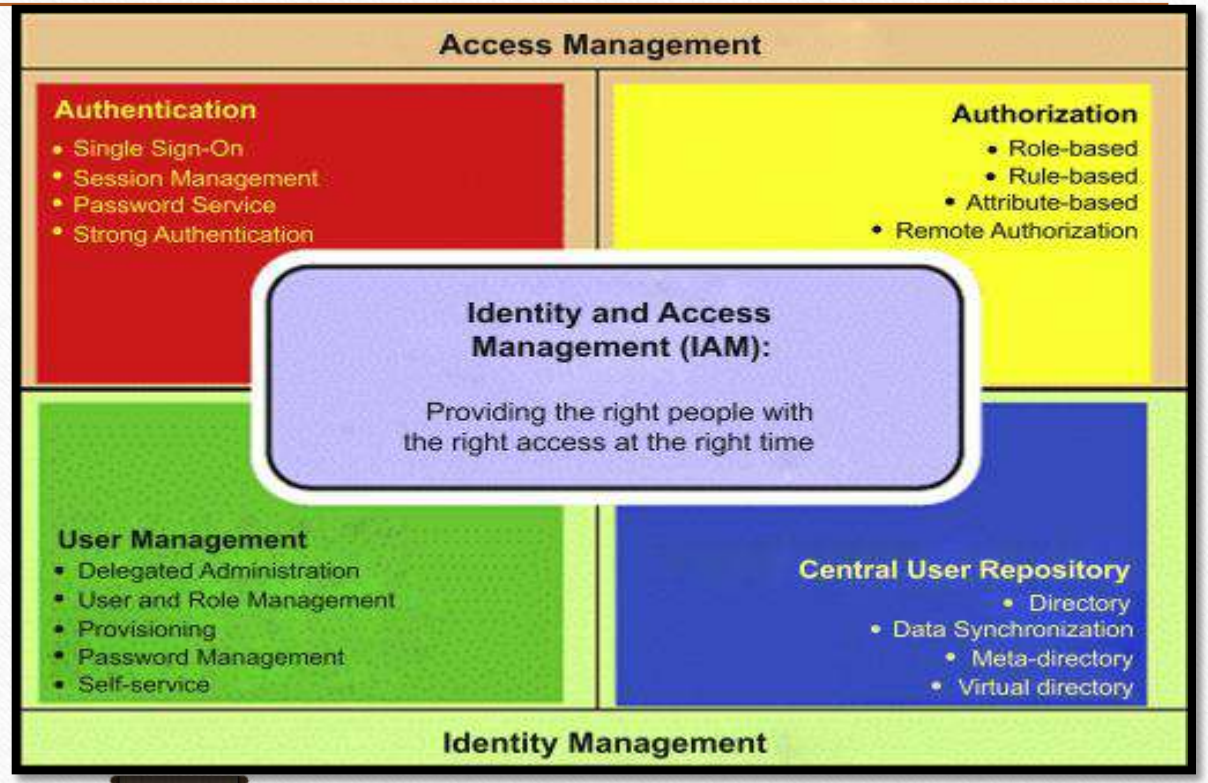
- Identity and Access Management (IAM) refers to the policies, processes, and technologies used to manage digital identities and control access to various resources and systems within an organization or application.
- It is a critical aspect of security and plays a crucial role in ensuring that only authorized individuals or entities can access sensitive data, applications, and systems.

Identity and access management

- The services and resources you want to access can be specified in IAM.
- IAM doesn’t provide any replica or backup.
- IAM can be used for many purposes such as, if one want’s to control access of individual and group access for your AWS resources.
- The AWS IAM is a global service.

Identity and access management

- It involves three main components:
- *Identity Management*
- *Access Management*
- *Auditing and Compliance*



Identity and access management

Identity Management:

- *Identification:* This involves establishing and verifying the identity of users, devices, or services that need access to resources.
- *Authentication:* The process of validating the claimed identities through methods such as passwords, biometrics, multi-factor authentication, or digital certificates.
- *User Provisioning:* Creating and managing user accounts, profiles, and access privileges within the organization or application.
- User Lifecycle Management: Managing the entire lifecycle of user identities, including creation, modification, suspension, and termination.

Identity and access management

Access Management:

- Authorization: Determining and enforcing the appropriate access rights, privileges, and permissions for authenticated identities to access specific resources or perform certain actions.
- Access Control: Implementing controls and policies that define who or what can access which resources, under what conditions, and with what level of access (e.g., read, write, execute).
- Role-Based Access Control (RBAC): Assigning access privileges based on the roles or responsibilities of users within the organization.
- Attribute-Based Access Control (ABAC): Granting access based on attributes associated with the user, the resource, and the environmental conditions.

Identity and access management

Auditing and Compliance:

- Monitoring and logging: Tracking and recording user activities, access attempts, and changes to identities and access rights for auditing and compliance purposes.
- Reporting and Analytics: Generating reports and analyzing user behavior, access patterns, and potential security incidents to enhance security and compliance.
- Compliance Management: Ensuring adherence to relevant regulatory requirements, industry standards, and organizational policies related to identity and access management.

Identity and access management

IAM Identities Classified As

- *IAM Users*
- *IAM Groups*
- *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.

Identity and access management

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.

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.

Identity and access management

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.

Identity and access management

IAM Features:-

Shared Access to your Account: A team working on a project can easily share resources with the help of the shared access feature.

Free of cost: IAM feature of the AWS account is free to use & charges are added only when you access other Amazon web services using IAM users.

Grant permission to the user: As the root account holds administrative rights, the user will be granted permission to access certain services by IAM.

Multifactor Authentication: Additional layer of security is implemented on your account by a third party, a six-digit number that you have to put along with your password when you log into your accounts.

Access control and authentication in cloud computing

Access Control:-

- Access control in cloud computing refers to the mechanisms and policies that govern what resources (e.g., virtual machines, storage, applications) users or systems can access and what actions they can perform on those resources.
- It involves implementing controls and rules to ensure that only authorized entities can access and interact with cloud resources.

Access control and authentication in cloud computing

Access Control:-

- Access Control in Cloud Computing refers to the ability to restrict access to information stored on the cloud.
- This allows companies to ensure their information is secured and helps minimize risk. Access Control is done through authentication processes which can include passwords, PINs, and multi-factor authentications.
- Effective access control in cloud computing environments is crucial for maintaining data security, ensuring regulatory compliance, and preventing unauthorized access or misuse of cloud resources.

Access control and authentication in cloud computing

There are various way for achieving Access Control:-

Identity and Access Management (IAM):

- Cloud service providers (CSPs) typically offer IAM services that allow organizations to manage user identities, authentication, and authorization.
- IAM services enable administrators to create and manage user accounts, assign roles or permissions, and control access to cloud resources.

Access control and authentication in cloud computing

There are various way for achieving Access Control:-

Role-Based Access Control (RBAC):

- RBAC is a widely adopted access control model in cloud computing. Roles are defined based on job functions or responsibilities within the organization.
- Permissions are then assigned to these roles, specifying the level of access and actions allowed on specific cloud resources.
- Users are assigned to one or more roles, inheriting the associated permissions.

Access control and authentication in cloud computing

There are various way for achieving Access Control:-

Attribute-Based Access Control (ABAC):

- ABAC is an access control model that makes access decisions based on attributes associated with the user, the resource, and the environment. Access policies are defined using a combination of these attributes, allowing for more granular and dynamic access control.

Access control and authentication in cloud computing

There are various way for achieving Access Control:-

Least Privilege:

- The principle of least privilege is widely adopted in cloud access control. Users and systems are granted the minimum level of access necessary to perform their intended functions, reducing the risk of unauthorized access or actions.

Access control and authentication in cloud computing

There are various way for achieving Access Control:-

Resource Policies:

- CSPs allow organizations to define resource-based policies that control access to specific cloud resources, such as virtual machines, storage buckets, or databases.
- These policies can specify actions allowed or denied, as well as the conditions under which access is granted or denied.

Access control and authentication in cloud computing

Authentication:-

- Authentication in cloud computing refers to the process of verifying the identity of users, devices, or services attempting to access cloud resources.
- It ensures that only legitimate and authorized entities can gain access to the cloud environment.
- Effective authentication mechanisms in cloud computing environments are essential for ensuring data security, preventing unauthorized access, and maintaining compliance with regulatory requirements

Access control and authentication in cloud computing

Authentication:-

There are various way for achieving Authentication:-

Identity Providers (IdPs):

- Cloud service providers (CSPs) often integrate with third-party identity providers (IdPs) or leverage their own identity management systems.
- IdPs are responsible for managing user identities, authenticating users, and providing authentication assertions or tokens to the cloud services.

Access control and authentication in cloud computing

Authentication:-

Authentication Methods:

- Username and Password: Traditional method where users provide a username and password to authenticate.
- Multi-Factor Authentication (MFA): In addition to a password, users must provide a second factor, such as a one-time code sent to their mobile device or a biometric authentication (e.g., fingerprint, facial recognition).
- Federated Identity: Users can authenticate using their existing credentials from a trusted identity provider (e.g., corporate directory, social media accounts) through protocols like SAML, OAuth, or OpenID Connect.
- Certificates and Keys: Digital certificates or cryptographic keys are used to authenticate systems, services, or applications accessing cloud resources.

Access control and authentication in cloud computing

Authentication:-

Single Sign-On (SSO):

- Cloud services often support SSO, which allows users to authenticate once and gain access to multiple cloud applications or services without having to re-authenticate for each one.

Access Tokens and Temporary Credentials:

- After successful authentication, cloud services typically issue access tokens or temporary credentials (e.g., session tokens, API keys) to authorize and grant access to specific resources or APIs within a limited timeframe.

Data Security in Cloud

Data security :-

- Data security is the process of safeguarding digital information throughout its entire life cycle to protect it from corruption, theft, or unauthorized access. It covers everything—hardware, software, storage devices, and user devices; access and administrative controls; and organizations' policies and procedures.
- Cloud data security protects data that is stored (at rest) or moving in and out of the cloud (in motion) from security threats, unauthorized access, theft, and corruption. It relies on physical security, technology tools, access management and controls, and organizational policies.

Data Security in Cloud

Data security :-

Data Security includes

- *Detecting and classifying structured and unstructured data.*
- *Implementing and monitoring access management controls at the file level.*
- *Data Transmission Flow*
- *Encryption Configuration*

Data Security in Cloud

Data security :-

The cloud data protection and security strategy must also protect data of all types. This includes:

- *Data in use: Securing data being used by an application or endpoint through user authentication and access control*
- *Data in motion: Ensuring the safe transmission of sensitive, confidential or proprietary data while it moves across the network through encryption and/or other email and messaging security measures*
- *Data at rest: Protecting data that is being stored on any network location, including the cloud, through access restrictions and user authentication*

Data Security in Cloud

Types of Data Security :-

- *Encryption*
- *Data Erasure*
- *Data Masking*
- *Data Resiliency*

Data Security in Cloud

Types of Data Security :-

- *Encryption:-*
- Data encryption is the use of algorithms to scramble data and hide its true meaning. Encrypting data ensures messages can only be read by recipients with the appropriate decryption key.
- This is crucial, especially in the event of a data breach, because even if an attacker manages to gain access to the data, they will not be able to read it without the decryption key.
- Data encryption also involves the use of solutions like tokenization, which protects data as it moves through an organization's entire IT infrastructure.

Data Security in Cloud

Types of Data Security :-

- *Data Erasure*

- There will be occasions in which organizations no longer require data and need it permanently removed from their systems. Data erasure is an effective data security management technique that removes liability and the chance of a data breach occurring.

Data Security in Cloud

Types of Data Security :-

- *Data Masking*
- Data masking enables an organization to hide data by obscuring and replacing specific letters or numbers.
- This process is a form of encryption that renders the data useless should a hacker intercept it.
- The original message can only be uncovered by someone who has the code to decrypt or replace the masked characters.

Data Security in Cloud

Types of Data Security :-

- *Data Resiliency*
- Organizations can mitigate the risk of accidental destruction or loss of data by creating backups or copies of their data.
- Data backups are vital to protecting information and ensuring it is always available.
- This is particularly important during a data breach or ransomware attack, ensuring the organization can restore a previous backup.

Technologies for Data security in Cloud

Technologies of Data Security :-

- Encryption Technologies:
- Authentication and Authorization Technologies:
- Network Security Technologies:
- Data Isolation and Segregation Technologies:
- Data Backup and Recovery Technologies:
- Security Monitoring and Logging Technologies:
- Secure Software Development Technologies:

Technologies for Data security in Cloud

Encryption Technologies:-

- *Symmetric Encryption (e.g., AES, 3DES):* Used to encrypt data at rest and in transit, providing confidentiality. AES is one of the most widely used encryption algorithms in cloud environments.
- *Asymmetric Encryption (e.g., RSA, ECC):* Used for secure key exchange, digital signatures, and authentication. RSA and Elliptic Curve Cryptography (ECC) are common asymmetric encryption algorithms.
- Key Management Systems: Specialized systems for securely generating, storing, rotating, and managing encryption keys used for data protection.

Technologies for Data security in Cloud

Authentication and Authorization Technologies::-

- Multi-Factor Authentication (MFA): Combines multiple factors (e.g., passwords, biometrics, security tokens) for stronger user authentication.
- Single Sign-On (SSO): Allows users to access multiple cloud services with a single set of credentials, enhancing usability and security.
- Identity and Access Management (IAM) systems: Centralized systems for managing user identities, access privileges, and authentication across cloud services.
- Role-Based Access Control (RBAC): Restricts access to cloud resources based on predefined roles and permissions, ensuring least privilege.

Technologies for Data security in Cloud

Network Security Technologies:-

- Virtual Private Networks (VPNs): Establish secure, encrypted tunnels between on-premises networks and cloud environments, protecting data in transit.
- Firewalls: Cloud-based firewalls control and monitor network traffic to and from cloud resources, blocking unauthorized access attempts.
- Web Application Firewalls (WAFs): Specialized firewalls that protect web applications hosted in the cloud from various attacks like SQL injection, cross-site scripting, etc.

Technologies for Data security in Cloud

Data Isolation and Segregation Technologies:-

- Virtualization (e.g., hypervisors, containers): Isolates workloads and data on shared physical resources, preventing unauthorized access between tenants.
- Multi-tenancy architectures: Logically separate data and resources for different customers or tenants on the same cloud infrastructure.

Technologies for Data security in Cloud

Data Backup and Recovery Technologies:-

- Cloud Storage Services (e.g., object storage, block storage): Durable and scalable storage solutions for backing up and archiving data in the cloud.
- Backup and Replication Services: Automated services for backing up data, creating snapshots, and replicating data across different cloud regions or providers for disaster recovery.

Technologies for Data security in Cloud

Security Monitoring and Logging Technologies:-

- Cloud Security Information and Event Management (SIEM): Collects and analyzes security logs, event data, and other information from cloud services to detect and respond to security incidents.
- Cloud Access Security Brokers (CASB): Provide visibility and control over cloud service usage, enforcing security policies and detecting potential threats.

Technologies for Data security in Cloud

Secure Software Development Technologies:-

- Static and Dynamic Application Security Testing (SAST, DAST): Analyze application code and runtime behavior to identify and remediate security vulnerabilities.
- Secure DevOps Practices: Integrate security practices throughout the software development lifecycle, from coding to deployment in the cloud.

Securing Private and Public Cloud Architecture

Private Cloud Architecture:-

- A private cloud is a cloud computing environment dedicated to a single organization or enterprise.
- It is typically hosted and managed within the organization's own data center or a third-party service provider's infrastructure.
- A private cloud is a cloud computing environment dedicated to a single organization, providing greater control and customization options.
- Securing private cloud architecture involves implementing various security measures and best practices to protect data, applications, and infrastructure from potential threats and vulnerabilities.

Securing Private and Public Cloud Architecture

Securing Private Cloud Architecture:-

- Physical Security: Implement robust physical security measures to protect the on-premises data center hosting the private cloud infrastructure. This includes access controls, surveillance systems, environmental controls, and secure equipment racks
- Network Security: Establish secure network segmentation, firewalls, and intrusion detection/prevention systems (IDS/IPS) to monitor and control network traffic. Implement virtual private networks (VPNs) for secure remote access and encrypt data in transit using technologies like SSL/TLS.

Securing Private and Public Cloud Architecture

Securing Private Cloud Architecture:-

- Identity and Access Management (IAM): Deploy a centralized IAM system to manage user identities, roles, and access privileges across the private cloud environment. Implement multi-factor authentication (MFA), role-based access controls (RBAC), and regular access reviews.
- Data Security: Encrypt sensitive data at rest and in transit using industry-standard encryption algorithms like AES. Implement key management systems for secure key generation, distribution, and rotation. Utilize data loss prevention (DLP) tools to monitor and protect sensitive data.

Securing Private and Public Cloud Architecture

Securing Private Cloud Architecture:-

- Virtualization Security: Secure the hypervisor and virtualization layer, which forms the foundation of the private cloud. Keep hypervisors and virtualization software up-to-date with the latest security patches. Implement secure configurations and hardening guidelines for virtual machines (VMs).
- Infrastructure Security: Regularly patch and update the underlying hardware, operating systems, and software components of the private cloud infrastructure. Implement secure configurations, enable logging and auditing, and conduct regular vulnerability assessments and penetration testing.

Securing Private and Public Cloud Architecture

Securing Private Cloud Architecture:-

- Compliance and Governance: Ensure compliance with relevant industry regulations and standards (e.g., HIPAA, PCI-DSS, GDPR) by implementing appropriate security controls, policies, and procedures. Establish governance processes for risk management, change management, and incident response.
- Monitoring and Logging: Implement centralized logging and monitoring solutions to collect and analyze security logs, events, and metrics from across the private cloud environment. Use security information and event management (SIEM) systems to detect and respond to security incidents.

Securing Private and Public Cloud Architecture

Public Cloud Architecture:-

- A public cloud is a cloud computing environment provided by third-party cloud service providers (CSPs) over the internet.
- The cloud resources are shared among multiple customers or tenants, and the infrastructure is owned and managed by the CSP.
- A public cloud is a cloud computing environment provided by third-party cloud service providers (CSPs) over the internet.
- Securing a public cloud architecture involves both the responsibilities of the CSP and the cloud customer.

Securing Private and Public Cloud Architecture

Securing Public Cloud Architecture:-

- Cloud Service Provider (CSP) Security: Evaluate and choose reputable CSPs with robust security measures, certifications (e.g., ISO 27001, SOC 2), and transparent security practices. Understand the shared responsibility model and the security controls provided by the CSP.
- Identity and Access Management (IAM): Utilize the IAM services provided by the CSP to manage access to cloud resources, implement least privilege principles, and enable multi-factor authentication (MFA) for all user accounts.

Securing Private and Public Cloud Architecture

Securing Public Cloud Architecture:-

- Data Security: Encrypt sensitive data at rest and in transit using CSP-provided encryption services or third-party encryption solutions. Implement key management best practices and follow data residency and compliance requirements.
- Network Security: Configure secure virtual private clouds (VPCs) or virtual networks within the public cloud environment. Implement network access control lists (ACLs), security groups, and network firewalls to control and monitor network traffic.

Securing Private and Public Cloud Architecture

Securing Public Cloud Architecture:-

- Infrastructure Security: Securely configure and harden cloud instances, containers, and serverless functions. Keep cloud resources up-to-date with the latest security patches and follow secure configuration guidelines provided by the CSP.
- Monitoring and Logging: Enable and configure logging and monitoring services provided by the CSP to capture and analyze security logs, events, and metrics. Integrate with third-party security information and event management (SIEM) solutions for centralized monitoring and incident response.

Securing Private and Public Cloud Architecture

Securing Public Cloud Architecture:-

- Compliance and Governance: Understand and adhere to the compliance and regulatory requirements applicable to your industry and data types. Leverage CSP-provided compliance services and tools, and implement additional controls as necessary.
- Third-Party Security: Assess and monitor the security posture of any third-party services, applications, or integrations used within the public cloud environment. Implement secure access controls and data protection measures for third-party integrations.

Metrics for Service Level Agreements(SLAs)

Service Level Agreements(SLAs):-

- *Service Level Agreements (SLAs) are contracts between a service provider and a customer, defining the level of service that the provider will deliver.*
- A service-level agreement (SLA) defines the level of service you expect from a vendor, laying out the metrics by which service is measured, as well as remedies or penalties should agreed-on service levels not be achieved.
- It is a critical component of any technology vendor contract.
- SLAs typically include various metrics to measure and evaluate the service performance.

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Availability:*
- *Response Time:*
- *Resolution Time:*
- *Performance:*
- *Capacity:*
- *Security:*
- *Support:*
- *Reporting and Monitoring:*
- *Penalties and Credits:*
- *Exit and Termination Clauses:*

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Availability:*
- This metric measures the uptime or accessibility of a service over a given period.
- Example: It is often expressed as a percentage, such as 99.9% availability, which translates to a maximum allowed downtime of approximately 8 hours and 45 minutes per year.

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Response Time:*
- This metric defines the maximum allowable time for a service provider to respond to a customer's request or incident.
- It can be measured as the time taken to acknowledge the request or the time taken to resolve the issue.
- Example: A support team may commit to acknowledging and responding to critical incidents within 15 minutes of being reported by the customer.

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Resolution Time:*
- This metric specifies the maximum time within which a service provider must resolve an issue or incident after it has been reported or acknowledged.
- Example: A software vendor may promise to resolve high-priority bugs or issues within 48 hours of being reported by the customer.

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Resolution Time:*
- This metric specifies the maximum time within which a service provider must resolve an issue or incident after it has been reported or acknowledged.
- Example: A software vendor may promise to resolve high-priority bugs or issues within 48 hours of being reported by the customer.

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Performance:*
- This metric measures the speed or throughput of a service, such as network bandwidth, data transfer rates, or transaction processing times.
- Example: A web hosting provider may guarantee an average page load time of less than 2 seconds for customer websites.

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Capacity:*
- This metric defines the maximum workload or usage that a service can handle, such as the number of concurrent users or the amount of data storage available.
- Example: A cloud storage service may offer a minimum storage capacity of 1TB per customer, with the option to scale up as needed.

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Security:*
- SLAs may include metrics related to security, such as the frequency of security audits, the time taken to address security vulnerabilities, or the level of encryption used for data protection.
- Example: A managed security service provider may conduct vulnerability scans and penetration tests on a quarterly basis to ensure the security of the customer's infrastructure.

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Support:*
- This metric covers the level of support provided by the service provider, including response times for support requests, availability of support channels (e.g., phone, email, chat), and the quality of support services.
- Example: A software vendor may offer 24/7 support with a guaranteed response time of 1 hour for critical issues, accessible via phone, email, and chat.

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Reporting and Monitoring:*
- SLAs may include metrics related to the frequency and quality of service reports, as well as the monitoring and logging capabilities provided by the service provider.
- Example: A managed service provider may provide daily reports on system performance, security events, and resource utilization, along with real-time monitoring and alerting capabilities.

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Penalties and Credits:*
- SLAs often define penalties or service credits that the provider must provide if they fail to meet the agreed-upon service levels.
- Example: A managed service provider may provide daily reports on system performance, security events, and resource utilization, along with real-time monitoring and alerting capabilities.

Metrics for Service Level Agreements(SLAs)

Metrics for Service Level Agreements(SLAs):-

- *Exit and Termination Clauses:*
- These metrics outline the terms and conditions for terminating the service agreement, including data retrieval, transition assistance, and any associated fees or penalties.
- Example: A data center hosting provider may offer a 60-day notice period for termination, along with assistance in migrating data to a new provider and a fee waiver for early termination in case of repeated SLA violations.

DevSecOps

DevSecOps:-

- DevSecOps, which is short for development, security and operations, is an application development practice that automates the integration of security and security practices at every phase of the software development lifecycle, from initial design through integration, testing, delivery and deployment.
- DevSecOps is a philosophy and practice that aims to integrate security practices into the entire DevOps process, from the initial design and development stages through deployment and operations.
- The primary goal of DevSecOps is to build security into the software development lifecycle (SDLC) rather than treating it as an afterthought.

DevSecOps

DevSecOps:-

- DevSecOps stands for development, security, and operations. It is an extension of the DevOps practice.
- Each term defines different roles and responsibilities of software teams when they are building software applications.
- *Development*
- *Security*
- *Operations*

DevSecOps

DevSecOps:-

Development :-

- Development is the process of planning, coding, building, and testing the application.

Security:-

- Security means introducing security earlier in the software development cycle. For example, programmers ensure that the code is free of security vulnerabilities, and security practitioners test the software further before the company releases it.

Operations:-

- The operations team releases, monitors, and fixes any issues that arise from the software.

DevSecOps

DevSecOps:-

The core principles of DevSecOps include:

- *Automation:* DevSecOps emphasizes the automation of security processes, such as security testing, vulnerability scanning, and compliance checks, to ensure that security measures are consistently applied throughout the development and deployment pipeline.
- *Collaboration:* DevSecOps promotes collaboration and shared responsibility among development, security, and operations teams. It breaks down the traditional silos between these teams, enabling them to work together closely from the beginning of the project.

DevSecOps

DevSecOps:-

The core principles of DevSecOps include:

- *Continuous Monitoring and Improvement:* DevSecOps advocates for continuous monitoring and improvement of security posture. Security is not a one-time activity but an ongoing process that requires constant vigilance and adaptation to emerging threats and vulnerabilities.
- *Shift-Left Security:* DevSecOps emphasizes shifting security practices to the left, meaning that security considerations are introduced as early as possible in the SDLC. This includes activities like threat modeling, secure coding practices, and security requirements gathering during the initial design and development phases.

DevSecOps

DevSecOps:-

The core principles of DevSecOps include:

- *Security as Code:* DevSecOps treats security configurations, policies, and controls as code, allowing them to be version-controlled, tested, and automatically deployed alongside the application code.
- By adopting DevSecOps, organizations aim to achieve faster and more secure software delivery, reduce the cost and effort associated with addressing security issues late in the SDLC, and foster a culture of shared responsibility for security across teams.