AWS Module 4

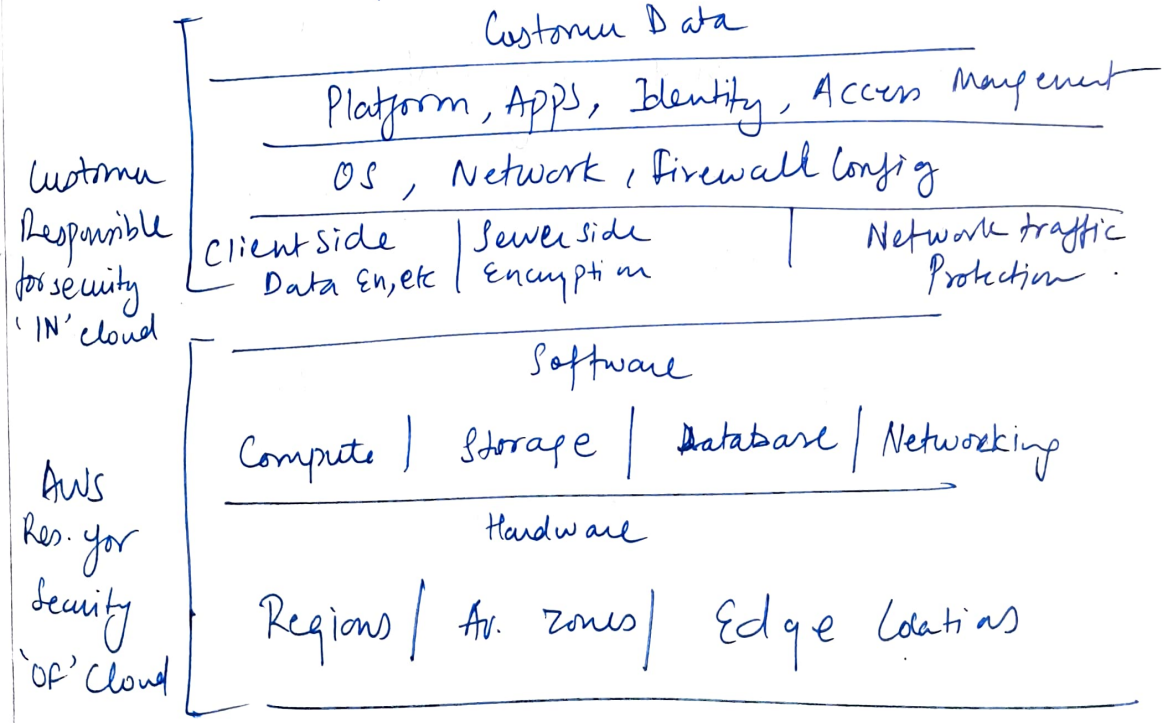
AWS cloud Security

Topics

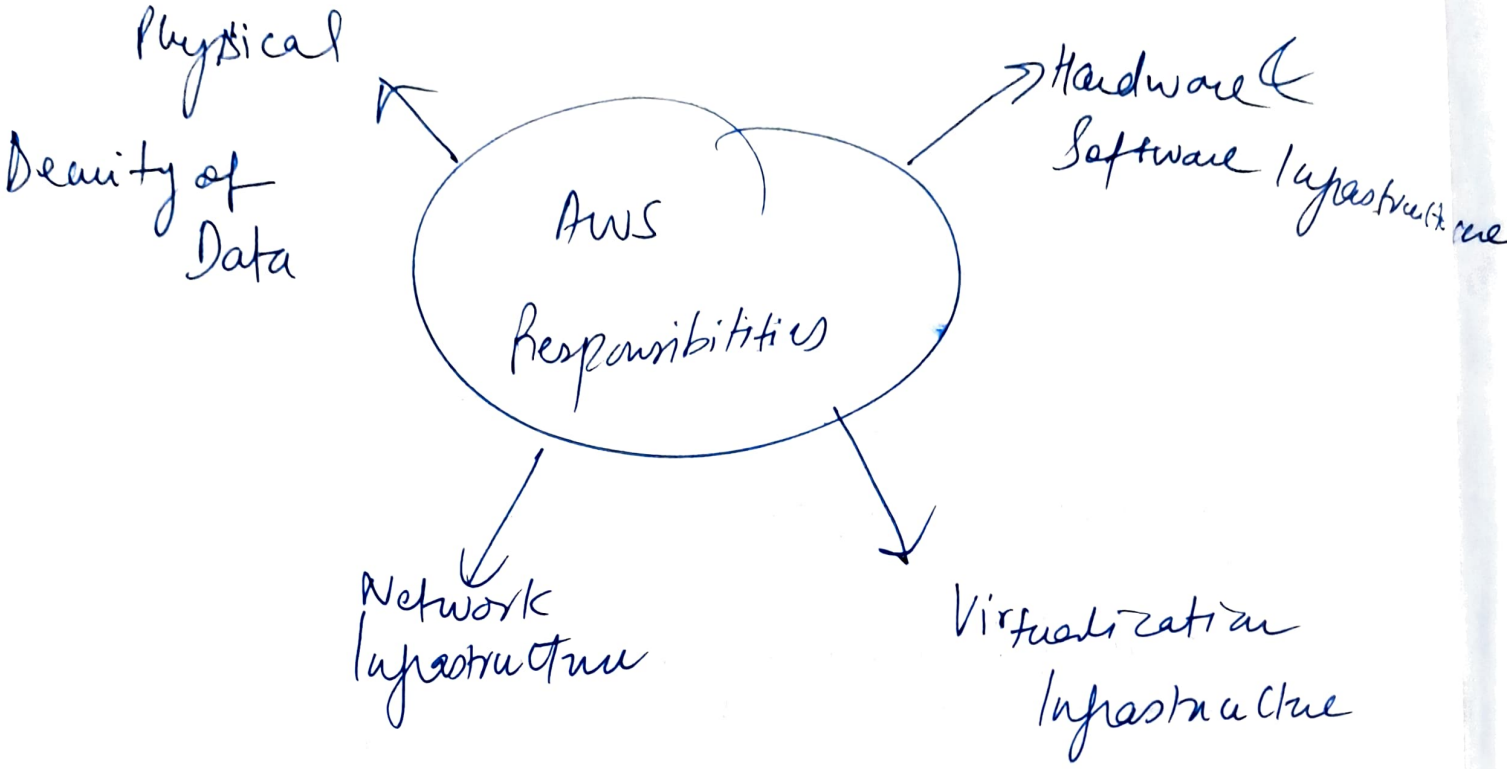
- AWS Shared responsibility model
- AWS Identity & Access Management (IAM)
- Securing a new AWS Account
- Securing Accounts
- Securing data on AWS
- Working to ensure Compliance.

(I) AWS Shared Responsibility Model

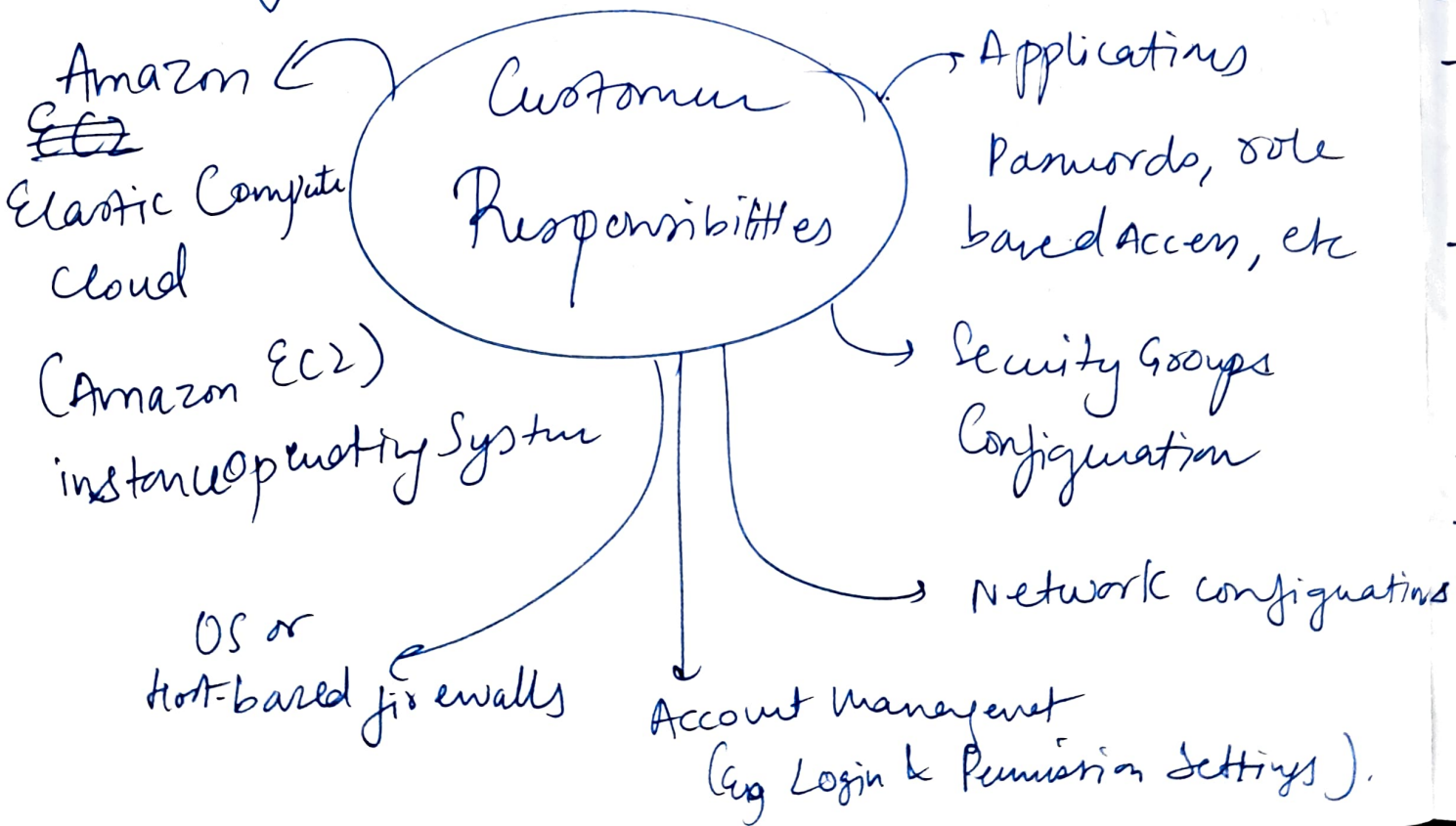
~~AWS is respon~~



→ Security of the cloud (by AWS) :-



→ Security In the cloud (by customer) :-



Examp Services

↳ Managed by Customer

Amazon EC2	Amazon EBS	Amazon VPC

↳ Managed by AWS

AWS Lambda	AWS RDS	AWS Elastic Beanstalk.

SaaS Examples → Aws Trusted Advisor, Aws Shield, Amazon Chime

II) AWS Identity Access Management (IAM)

→ Allows you to define users & the types of access that they will be allowed to have.

→ Use IAM to manage access to AWS resources —

- A resources is an entity in an AWS ~~Service~~ Account that you can work with Ex Amazon EC2, S3

→ Example: Control who can terminate EC2 instances.

→ Defined fine-grained access rights

↳ Who can access

↳ which resources can be accessed

↳ How resources can be Accessed.

→ No cost AWS Account feature.

→ IAM : Essential Components

- IAM User: A person / Application that can authenticate with an AWS Account
- IAM Group: Collection of IAM Users that are granted identical authorization.
- IAM Policy: Document that defines which resources can be accessed & the level of access to each resource.
- IAM Role: Useful mechanism to grant a set of permissions for making AWS Service requests.

→ Authenticate as an IAM User to gain Access:

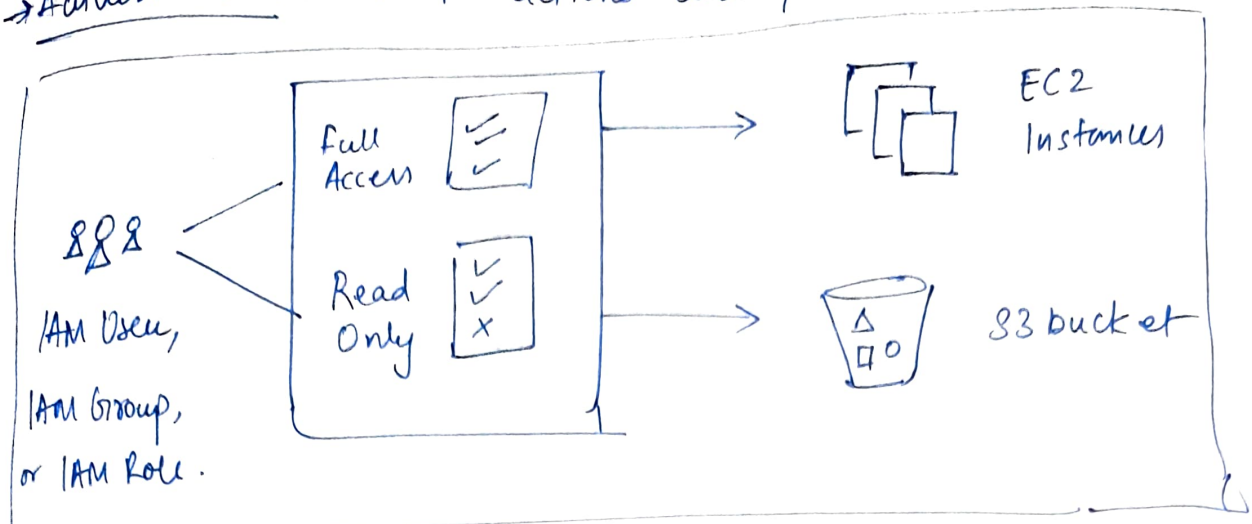
When you define an IAM User, you select what type of access the user is permitted to use.

1) Programmatic Access: — for AWS CLI & AWS Tools & SDKs
   ↳ Authenticate Using
   - Access key ID
   - Secret Access key
   ↳ Provides AWS CLI & AWS SDK Access

2) AWS management Console Access: — for AWS management console.
   ↳ Authenticate using:
   - 12 digit Account ID or alias
   - IAM Username
   - IAM Password.
   ↳ When enabled, Multi Factor Authentication (MFA) prompts for an authentication code.

In addition to username & password, MFA asks for an authentication code as well.

→ Authorization : What actions are permitted?



After a user/App^n is connected to AWS, what are they allowed todo?

→ Assign permissions by creating IAM policy

→ Permissions determine which resources & operations are allowed:

↳ All permissions are implicitly denied by default

↳ If something is explicitly denied, it's never allowed.

→ Best practice : Follow the principle of least Privilege

NOTE → Scope of IAM service configurations is global. Setting apply across all AWS regions.

→ IAM Policy

- IAM Policy is a document written using JS Object Notation
- A policy list the permissions that allow/deny access to services in AWS.

IAM Policy → Identity based Policies:

→ Resource based Policies:

1.) Identity-based Policies

- Attach a policy to any IAM entity — An IAM user/group/role
- Policy specify Actions that may/may not be performed by an entity.
- A single policy can be attached to multiple entities
- A single entity can have multiple policies attached to it.

2.) Resource-based Policies

- Attached to a resource (like a S3 buckets).

→ Example

- Explicit allow gives users access to a specific DynamoDB table & Amazon S3 buckets.

- Explicit deny ensures that the users cannot use any other AWS actions or resources other than that table & those buckets.

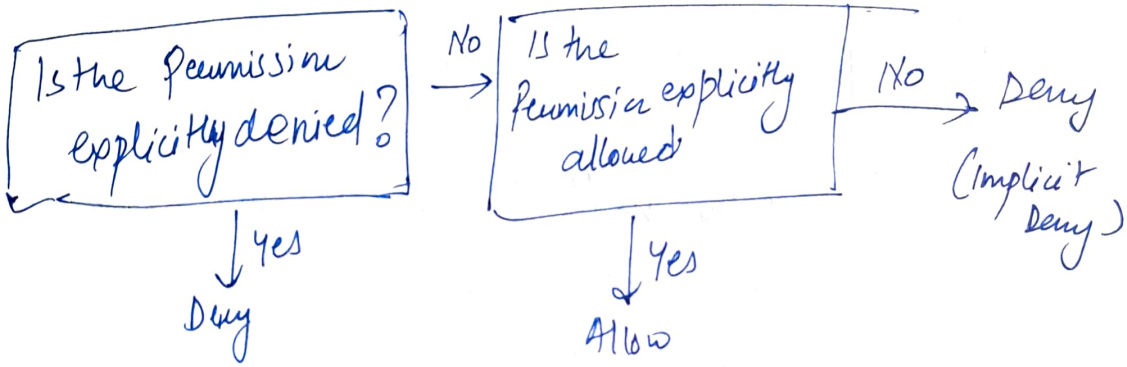
> An Explicit deny statement takes precedence over an allow statement

i.e. If same resource is allowed & denied somewhere differently, denied always wins.

2.) Resource-based Policies

- Attached to a resource (not a single user/group/role)
- Characteristics of resource-based policies —
  - ↳ Specifies who has access to the resource & what actions they can perform on it
  - ↳ The policies are inline only, not managed.
- Resource-based policies are supported by some AWS services.

→ IAM Permissions



→ IAM Group

- Collection of IAM users
- A Group is used to grant the same permissions to multiple users. (by attaching ~~multip~~ IAM Policy/policies to the group.
- Users can belong to multiple groups
- There is no default group
- Groups cannot be nested.

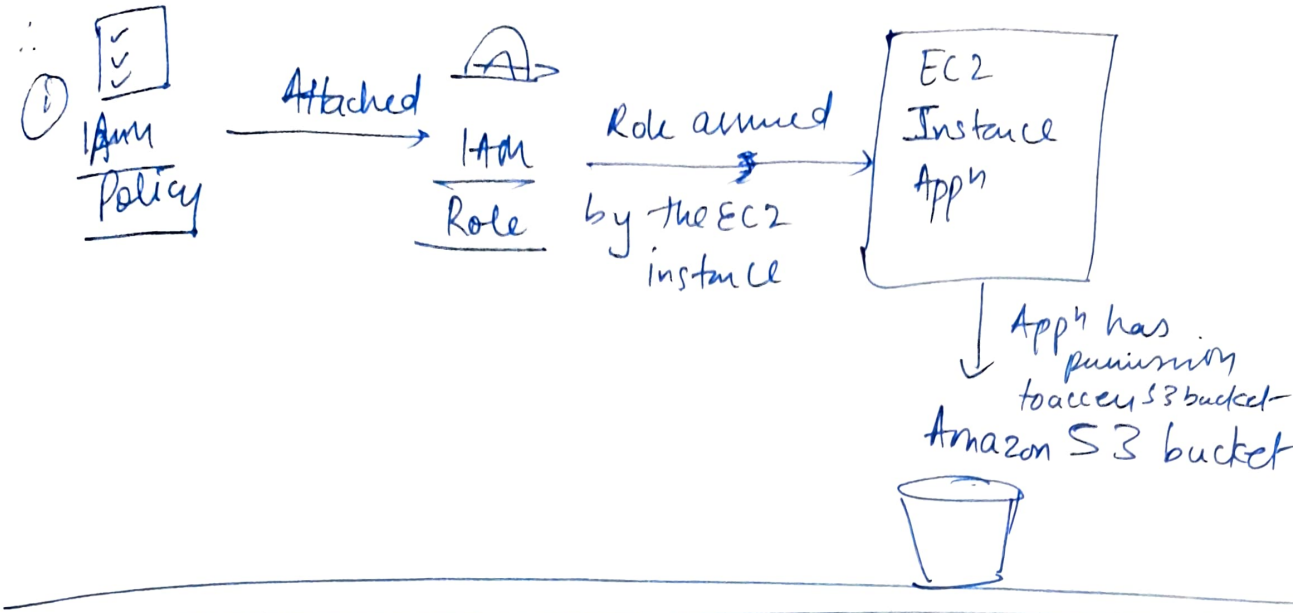
→ **IAM Role** : An identity with specific permissions

- Similar to IAM user — Attach permissions & policies to it
- Different from an IAM user.
  - Not uniquely associated with one person
  - Intended to be assumable by a person, application, or service.
- Roles provide temporary security credentials.
- Example of how IAM roles are used to delegate Access:
  - Used by an IAM user in the same AWS account as role.
  - Used by an AWS service — like EC2 - in same account as the role.
  - Used by an IAM user in a different AWS account than that role.

Example use of IAM Role.

Scenario:- App^n running on EC2 instance needs access to an S3 bucket.

Soln:
- Define an IAM policy that grants access to the S3 bucket.
- Attach policy to a role
- Allow the EC2



(III) Securing a New AWS Account

→ Best Practice :- [DO NOT use the AWS account root user except when necessary]

(Access to Acc. root user requires logging in with the email address (and password) that you used to create the account.)

→ Example actions that can only be done with the account user:

- → Update the account root user password.
- → Change the AWS support plan
- → Restore the IAM user's permissions
- Change account settings (for example, contact information, allowed Regions).

Account root User	IAM
- Privilege cannot be controlled	- Integrate with other AWS resources
- Full access to all resources	- Identity federation
	- Secure access for applications
	- Granular Permissions.

~~Secure Account root User~~

Step 1: Stop Using account root User as soon as possible.

(Root User Account)

- Create IAM User for yourself
- Create IAM Group, give it full rights and the IAM user to it.
- Disable & Remove your account root user access keys
- Enable a password policy

Step 2: Multi Factor Authentication (MFA)

(MFA)

- Require MFA for your account root user for all IAM Users.
- Options for retrieving the MFA token -
  - Virtual MFA-compliant applications:
    - Google Authenticator
    - Authy Authenticator
  - U2F security key devices:
    - Ex Yubikey
  - Hardware MFA options:
    - Key fob or display card offered by Gemalto.

Step 3 : Use AWS CloudTrail → Who, what, when, where of API interactions

(AWS CloudTrail) – CloudTrail — Tracks user activity on your account
↳ Logs all API requests to resources in all supported services your account.

- Basic AWS CloudTrail event history is enabled by default & it's free (Contains management event data on last 90 days of activity)
- To enable logs beyond 90 days & enable specified event alerting, create a trail.

Step 4 : Enable a billing report — such as AWS Costs & Usage report

(Billing Reports)

- It provides information on your use of AWS resources & estimated costs for that use.
- AWS delivers the reports to an Amazon S3 bucket that you specify (Report is updated atleast once a day)
- The AWS cost & Usage Report tracks your AWS usage & provides estimated charges associated with your AWS account (either hr or day by the

(IV) Securing Accounts : AWS Organisations

- AWS Organisations enables you to consolidate multiple AWS Accounts so that you centrally manage them.

- Security features of AWS Organizations:
  - Group AWS Accounts into Organizational Units (OUs) & attach different access policies to each OU.
  - Integration & support for IAM : Permissions to a user are the intersection of what is allowed by AWS Organizations & what is granted by IAM in that account.
  - User service control policies : To establish control over the AWS services & API actions that each AWS account can access.

Securing Accounts : Service Control Policies

- Service Control Policies (SCPs) offer centralized control over accounts: Limit permissions that are available in an account that is part of an organization.
- Ensures that accounts comply with access control guidelines.
- SCPs are similar to IAM permissions policies:
  - They use similar Syntax
  - However, a SCP never grants permissions
  - Instead, SCPs specify the maximum permissions for an organization.

AWS Key Mangement Service (AWS KMS)

Features:

- Enables you to create & manage encryption keys.
- Enables you to control the use of encryption across AWS Services & in your App's.
- Integrate with AWS CloudTrail to log all keys usage.
- Uses Hardware Security (HSMs) that are validated by Federal Information Processing Standards (FIPS) 140-2 to protect keys.

Amazon Cognito

Features:

- Adds User sign up, sign in & access control to your web & mobile App^ns.
- Scales to millions of Users.
- Supports sign-in with social identity providers, such as Facebook, Google, Amazon, etc. & Enterprise Identity Providers like Microsoft Active Directory via Security Assertion Markup Language (SAML) 2.0. (used by Amazon Cognito)

AWS Shield

Features:

- Managed distributed denial of Service (DDoS) protection Service.
- Safeguards app^ns running on AWS.
- Provides always-on detection & automatic inline mitigations.
- AWS Shield Standard enabled for at no additional cost. AWS Shield Advanced is an optional paid Service
- Use it to minimize app^n downtime & latency.

(V) Securing data on AWS

→ Encrypting of data at rest

- Encryption encodes data with a secret key, which makes it unreadable.
  - Only people with secret key can decode the data.
  - AWS KMS can manage your secret keys.
- AWS supports encryption of data at rest.
  - Data at rest = Data stored physically (on disk or tape).
  - You can encrypt data stored in any service that is supported by AWS KMS including :-
    - ↳ Amazon S3
    - ↳ Amazon EBS
    - ↳ Amazon EFS
    - ↳ Amazon RDS.

→ Encryption of data in transit

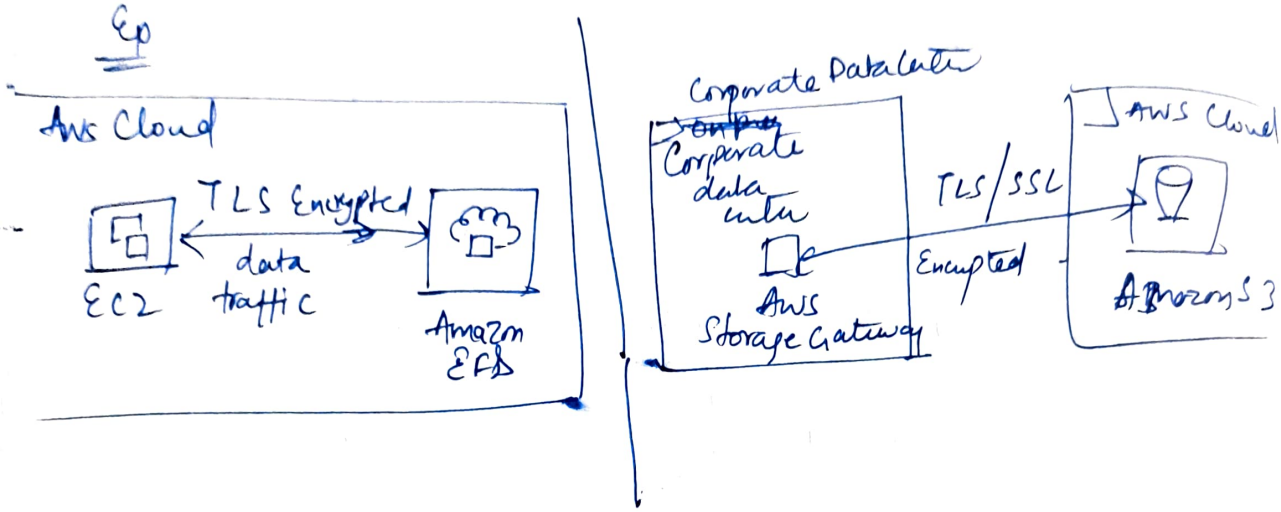
- Encryption of data in transit = data moving across a network.
- Transport Layer Security (TLS) — formerly SSL is an open standard protocol.
- AWS Certificate Manager Provides a way to manage, deploy & renew TLS or SSL certificates.

Provision & manage deployment of SSL & TLS certificates

- Secure HTTP (HTTPS) creates a secure tunnel.
  ↳ Uses TLS or SSL for the bidirectional exchange of data.

- AWS services support data in transit encryption

Eg



Securing Amazon S3 buckets & Objects

- Newly created S3 buckets & objects are private & protected by default
- When use cases require sharing data objects on Amazon S3 —
  - Its essential to manage & control data access
  - Follow permissions that follow principle of least privilege & consider using Amazon S3 encryption

- Tools & Options for controlling access to S3 data include :-

  - Amazon S3 Block Public Access feature : Simple to use.
  - IAM policies : Good option when user can authenticate using IAM.
  - Bucket Policies.
  - Access Control Lists (ACLs) : A Legacy access control mechanism. (Older than IAM so less used)
  - AWS Trusted Advisor bucket permission check : A free feature.

(VI) Working to Ensure Compliance

→ AWS Compliance Programs

- Customers are subject to many different security & compliance regulations & requirements.
- AWS engages with certifying bodies & independent auditors to provide customers with detailed info about the policies, process & controls that are established & operated by AWS.
- Compliance programs can be broadly categorized :

Certifications & Attestations	Laws & Regulations & privacy	Alignments & Frameworks.
- Assessed by 3rd party, Indepedent auditor Ex ISO 27001, 27017, 27018, ISO/IEC 9001	- AWS provides security features & legal agreements to support compliance - Ex. EU General Data Protection Regulation (GDPR), HIPAA	- Industry- or func" specific security/ compliance req. Ex Center for internet security (CIS), EU-US privacy Shield.

AWS Config

→ Service to Assess, audit & evaluate the configurations of AWS resources.

→ Use for continuous monitoring of configurations.

→ Automatically evaluate recorded configurations versus desired configurations.

→ Review configuration changes

→ View detailed Configuration histories.

→ Simplify compliance auditing security analysis.

AWS Artifact

→ Provides on demand downloads of AWS security & compliance documents.

→ Its a resource for compliance-related information.

→ Provide access to security & compliance reports, & select online agreements.

→ Can Access Example downloads:

- AWS ISO certifications
- Payment card Industry (PCI) & Service Organization Control (SOC) Reports.

→ Access AWS Artifact directly from the AWS Management Console.

- Under Security, Identity & Compliance, click Artifact.