Day 9/13

Module 9 - Security

Date
DELTA Pg No.

#1 Introduction

Authentication: verifying the identity of a user or entity through credentials.

Authorization: Granting authenticated users with certain access rights and permissions.

Data privacy and protection: Maintains customer trust and prevents fraud.

→ AWS Shared Responsibility model means AWS secures the cloud infrastructure while customers are responsible for securing their data, configurations and access within the cloud.

#2 Preventing Unauthorised Access.

AWS account root user: Access and control any resource in the account

Use strong password and MFA.

Principle of Least privilege: A user is granted access only to what they need.

Date
DELTA Pg No.

AWS IAM

Root User
User
Groups
Policies
Roles.

AWS Roles

- Associated permission
- Allow or deny
- Assumed for temporary amounts of time.
- No username or password.

IAM (Identity and Access Management) lets you securely control who can access AWS resources and what actions they can perform.

Components:

- Users: Individual Identities (for people or apps).
- Groups - Collection of users with common permissions.
- Roles - Temporary access with permissions (used by services, apps, cross-account)
- Policies - JSON documents that define permissions (Allow / Deny)

Policy Basics

→ Written in JSON.
→ Define:
  - Effect (Allow / Deny)
  - Action.
  - Resource.

- Explicit Deny always overrides Allow.

Authentication & Security

- MFA (Multi-Factor Authentication) → Extra security layer
- Root User → Has full access; avoid using it.
- Enable MFA on root account
- Use least privilege principle.

Access Types

- programmatic access - Access key + Secret key
- Console access → Username + Password.

IAM is global, not region-specific.

AWS IAM Identity Center - provides centralized single sign-on (SSO) access across multiple AWS accounts and applications using federated identity management

AWS secrets Manager : Securely stores, manages and automatically rotates sensitive information like database credentials and API keys

AWS Systems Manager - Centrally manages and automates operations (like patching and configuration) across AWS.

Date
DELTA Pg No

#3 Protecting Networks and Applications

DoS Attacks (Denial of Service)

In a DoS attack, an attacker floods a web application with excessive network traffic.

DDoS – Distributed Denial of Service (DDoS) = Attack where multiple compromised machines (botnet) flood your application with traffic to exhaust resources and make it unavailable.

EX :- UDP Flood

→ Attacker sends small requests with fake return address (victim's IP)
→ Third-party servers send massive responses to victim.
→ Result → Network overwhelmed.

How AWS Defends against DDoS.

1. **Security Groups**
   - Act as network-level firewall
   - Allow only approved protocols / ports
   - Block unwanted traffic (e.g. UDP if not required)
   - Operate at AWS infrastructure level (not just OS firewall)
   - Good for filtering unwanted traffic before it hits EC2

Date
DELTA Pg No.

Note: Allow only specific traffic → security groups
Restrict protocol/port → security groups.

(2) AWS Shield Standard (Free, Built-in)
- Automatically protects against common DDoS attacks
- Included with:
  - Elastic Load Balancer (ELB)
  - CloudFront
  - Route 53
- NO Extra cost

(3) AWS WAF (Web Application Firewall)
- Filters HTTP/HTTPS traffic
- Blocks malicious patterns (IP, SQL injection, bots)
- Works at application layer.
- Often used with CloudFront or ALB (Application Load Balancer).

(4) AWS Shield Advanced (Paid)
- Advanced DDOS protection.
- Detailed Attack Diagnostics.
- Protection against Sophisticated attacks
- Cost protection for scaling during attack.

Date
DELTA Pg No.

#4 Protecting Data

Encryption: securing data in a way that only authorized parties can access it.

→ Protect PII & credit card Data
→ Avoid legal + trust issues.
→ Based on lock & key model (same key = symmetric)

Encryption at Rest (Stored Data)

- Amazon S3
  → New buckets → encryption ON by default.
  → New objects → automatically encrypted

- Amazon EBS
  → Volumes + snapshots encrypted.
  → Boot + data volumes both supported

- Amazon DynamoDB
  - Server-side encryption enabled by default.
  - Uses AWS KMS keys

AWS Key Management Services (KMS)

→ Creates & manages cryptographic keys
→ Fine-grained IAM control
→ Keys can be disabled

→ Keys never leave KMS.

Encryption in Transit (Data Moving).
- Uses TLS (newer than SSL)
- HTTPS = HTTP secured by TLS
- Protects data over network.

AWS Certificate Manager (ACM).
- Manages SSL/TLS certificates
- Used to secure AWS + on-prem services.

Amazon Macie: ML-based service that automatically discovers and monitors sensitive data stored in Amazon S3 to support security and compliance. (Rest)

#5 Detecting and Responding to Security Incidents

Amazon Inspector
→ Runs automated security assessments.
→ Finds security best practices deviations
→ Detects Amazon EC2 exposures.
→ Finds vulnerable software installations

Date
DELTA Pg No

Amazon Guard Duty
- continuous monitoring
- AI/ML powered threat management

Amazon Detective
→ simplified, automatic security Investigations
→ Interactive threat visualisations.
→ Generative AI powered insights.

Amazon security Hub
→ one comprehensive security view
→ Automatic, efficient monitoring
→ Actionable groupings of insights

Scan → Inspector
Detect → Guard Duty
Investigate → Detective (Root cause)
Dashboard → security Hub.