DATE 31/12/21

Day 24/100

Security & Compliance

AWS Shared Responsibility Model

- AWS responsibility - Security of the Cloud
  - Protecting infrastructure (hardware, software, facilities & network) that runs all the AWS services
  - Managed service like S3, DynamoDB, RDS etc.
- Customer responsibility - Security in the cloud
  - For EC2 instance, Customer is responsible for management of the guest OS (including security patches & updates), firewall & network configuration, IAM
  - & encrypting application data

CUSTOMER Responsibility for Security - IN the Cloud	CUSTOMER DATA		
	Platform, Application, Identity & Access Management		
	Operating System, Network & Firewall Configuration		
	Client-Side Data Encry & Data Integrity Authentication	Server-Side Encry File System And/OR DATA)	Networking Traffic Protection (Encry, Integrity, Identity)
AWS Responsibility for Security 'OF' the Cloud	SOFTWARE		
	COMPUTE	STORAGE	Database	Networking
	Hardware/AWS Global Infrastructure		
	Regions	Availability Zones	Edge Locations

DATE 31/12/21

DDOS Protection on AWS

- AWS Shield Standard: protects against DDOS attack for your website and application, for all customers at no additional costs.
- AWS Shield Advanced: 24/7 premium DDos protection
- AWS WAF: Filter specific requests based on rules.
- CloudFront & Route53:
  - Availability protection using global edge network.
  - Combined with AWS Shield, provides attack mitigation at the edge
- Be ready to scale - leverage AWS Auto Scalling.

⇒ AWS Shield

- AWS Shield Standard:
  - Free service that is activated for every AWS Customer
  - Provides protection from attacks such as SYN/UDP Floods, Reflection attacks & other layer 3/layer 4 attacks.
- AWS Shield Advanced:
  - optional DDOS mitigation service ($3000 per month per organization)

DATE 31/12/21

- Protect against more sophisticated attack on Amazon EC2, Elastic Load Balancing [ELB], Amazon CloudFront, AWS Global Accelerator, & Route 53.
- 24/7 access to AWS DDoS response team [DRP].
- Protect against higher fees during usage spikes due to DDoS.

⇒ AWS WAF - Web Application Firewall

- Protects your web application from common web exploits (Layer 7)
- Layer 7 is HTTP (vs layer 4 is TCP)
- Deploy on Application Load Balancer, API Gateway, CloudFront

- Define web ACL (web Access Control List):
  - Rules can include IP addresses, HTTP headers, HTTP body or URI strings
  - Protects from common attack - SQL injection & Cross-Site Scripting (XSS)
  - Size Constraints, geo-match (block countries)
  - Rate-based rules (to count occurrences of events) - for DDoS protection

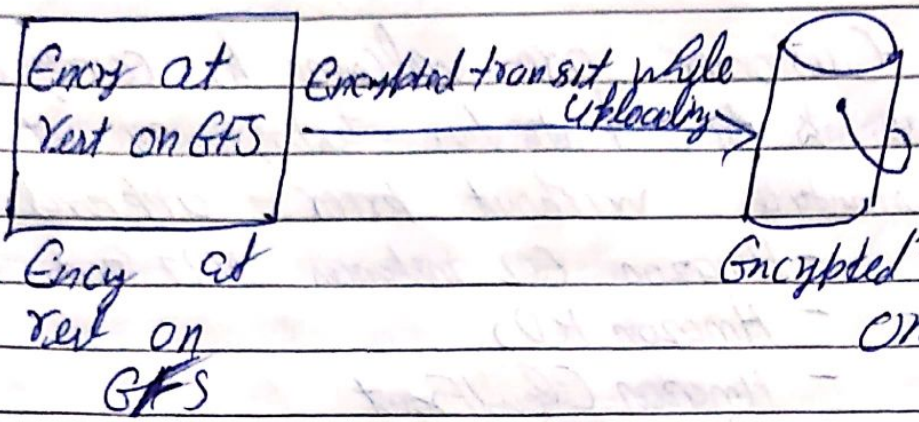
DATE 31/12/21

Penetration Testing on AWS Cloud

- AWS Customer are welcome to carry out security assessments or penetration testing against their AWS infrastructure without prior approval for 8 services
  - Amazon EC2 instances, NAT Gateways, & ELB
  - Amazon RDS
  - Amazon CloudFront
  - Amazon Aurora
  - Amazon API Gateways
  - AWS Lambda & Lambda Edge functions
  - Amazon Lightsail resources.
  - Amazon Elastic Beanstalk environments.

⇒ Prohibited Activities
  - DNS zone walking via Amazon Route 53 Hosted zones
  - Denial of service (DOS), Distributed Denial of Service (DDOS), Simulated DOS, Simulated DDOS.
  - Port flooding
  - Protocol flooding
  - Request flooding (login request flooding, API request flooding)

Data at rest v/s Data in transit



- At rest: data stored or archived on a device
  - On a hard disk, on a RDS instance, in S3 Glacier Deep Archive etc.
- In transit (in motion): data being moved from one location to another
  - Transfer from On-premises to AWS, EC2 to DynamoDB etc.
  - Means data transferred on the network.
- We want to encrypt data in both states to protect it!
- For this we leverage encryption keys.

AWS KMS (Key Management Service)

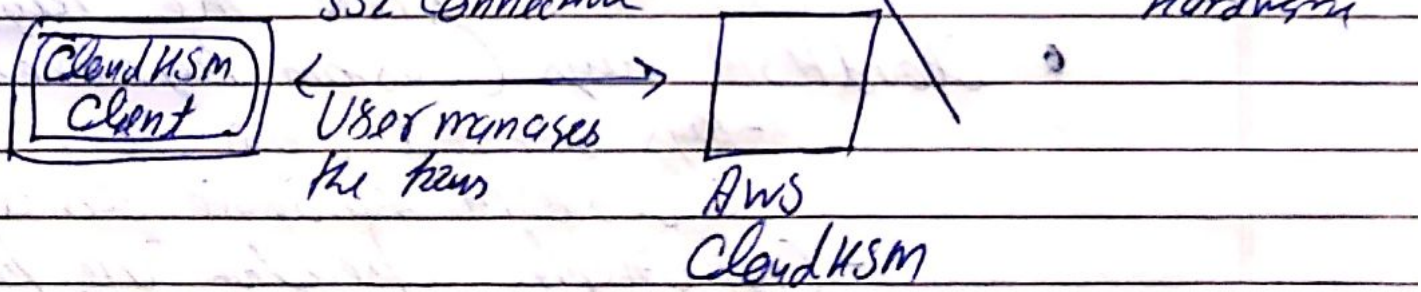
- Anytime you hear "encryption" for an AWS service, it's most likely KMS.

DATE 31/12/21

- KMS = AWS manages the encryption key for us.
- Encryption opt-in:
  - EBS volumes: encrypt volumes
  - S3 buckets: Server-Side encry. of objects
  - Redshift database: encry. of data
  - RDS database: encry of data
  - EFS drives: encry of data
- Encryption automatically enabled
  - CloudTrail Logs
  - S3 Glacier
  - Storage Gateway

CloudHSM

- KMS => AWS manages the software for encry.
- CloudHSM => AWS provisions encry hardware
- Dedicated Hardware (HSM = Hardware Security Module)
- You manage your own encryption key entirely (not AWS)
- HSM device is tamper resistant, FIPS 140-2 level 3 compliance



DATE 31/12/21

Types of Customer Master key : CMK.

- Customer Managed CMK:
  - Create, manage and used by the customer can enable or disable
  - Possibility to rotate Policy (new key generated every year, old key preserved)
  - Possibility to bring-your-own-key.

- AWS managed CMK:
  - Create, managed & used on the Customer behalf by AWS.
  - Used by AWS services (aws/s3, aws/ebs, aws/redshift)

- AWS Owned CMK:
  - Collection of CMKs that an AWS service own and manages to use in multiple accounts
  - AWS can use those to protect resource in your account (but you can't view the keys)

- CloudHSM keys (Custom keystore):
  - Keys generated from your own CloudHSM hardware device
  - Cryptographic operation are performed within the CloudHSM cluster

DATE 31/12/21

AWS Certificate Manager (ACM)

- Lets you easily provision, manage & deploy SSL/TLS Certificates
- Used to provide in-flight encryption for websites [HTTPS]
- Supports both public & private TLS certificates
- Free of charge for public TLS certificates
- Automatic TLS certificates renewal.
- Integrations with Cloud TLS certificates on)
  - Elastic Load Balancers.
  - CloudFront Distributions
  - APIs on API Gateway