* Amazon S3 Security *:

- With SSE-C, the encryption happens in AWS and you have full control over the encryption keys.
- With SSE-KMS, the encryption happens in AWS and the encryption keys are managed by AWS but

you have full control over the rotation policy of the encryption key. Encryption keys stored in AWS.

With client-side encryption, you have to do the encryption yourself and you have full control over the encryption keys. You perform the encryption yourself and send the encrypted data to AWS. AWS does not know your encryption keys and cannot decrypt your data.

CORS (Cross-Origin Resource Sharing) defines a way for client web applications that are located in one domain to interact with resources in a different domain.

S3 Access logs log all the requests made to S3 buckets and Amazon Athena can then be used to run serverless analytics on top of the log files.

S3 Pre-signed URLs are temporary URLs that you generate to grant time-limited access to some actions in your S3 bucket.

Eg: Policy that dB backups must be retained for 4 years: Glacier vaults with vault lock policies.

Amazon S3 automatically encrypt new objects using server-side encryption with S3-Managed Keys (SSE-S3)

- MFA delete forces users to use MFA codes before deleting S3 objects. Its an extra level of security to prevent accidental deletions.
- Data & files stored in S3 buckets. Some of these files need to be kept for a predefined period of time and protected from being overwritten and deletion according to company compliance policy - use S3 object lock - Retention compliance mode.
- Legal hold S3 object lock configuration allows you to prevent an object or its version from being overwritten or deleted indefinitely and gives you the ability to remove it manually.