AWS KMS (Key Management Service)

KMS

OVERVIEW

- Fully managed encryption service by AWS.
- Helps create, manage, and control cryptographic keys
- Integrated with over 70 AWS services (e.g., S3, EBS, RDS, Lambda.
- dUses FIPS 140-2 validated HSMs to protect your keys

KEY FEATURES

- Create & manage keys (Customer Managed Keys - CMKs)
- Automatic key rotation for better security
- Grants and Key policies for fine-grained access control
- Audit trail via AWS CloudTrail

KMS

key Types

- Customer Managed Keys (CMKs) – You manage lifecycle & permissions
- AWS Managed Keys – Created & managed automatically by AWS
- AWS Owned Keys – Used by AWS services, not visible to users

ENCRYPTION

Use Cases

- Encrypt data at rest (S3, EBS, RDS)
- Encrypt secrets and environment variables (Lambda, Secrets Manager)
- Sign & verify digital signatures
- Encrypt data in custom applications using the KMS API

SECURITY AND COMPLIANCE

- Integrated IAM access control
- HSM-backed key storage
- Audit logging with CloudTrail
- Compliance with PCI-DSS, HIPAA, FedRAMP, FIPS 140-2