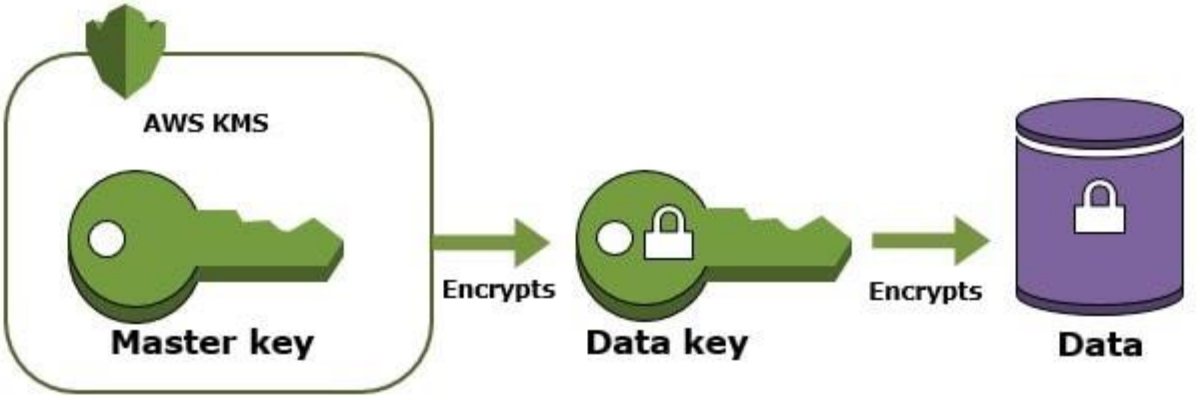
AWS Key Management Service (AWS KMS) for Data Encryption

AWS provides over a hundred plus services which include storage, networking, database, application services, and many more. Out of these services, AWS KMS **Key Management Service** is a useful and very beneficial service while dealing with sensitive data and it also makes it easy for you to create and manage cryptographic keys.

Overview Of AWS KMS

AWS KMS is a safe and resilient service that uses hardware security protocols that are tested or are in the process of being tested to protect our keys. AWS Key Management Service provides a highly available key storage, management, and auditing solution for you to encrypt data within your own applications and control the encryption of stored data across AWS services.



Features of AWS KMS

- It is an easy way to control and access your data using managed encryption.
- With AWS Key Management Service, the process of key management is reduced to a few simple clicks.
- It is also integrated with other AWS services including Amazon EBS, Amazon S3, and Amazon RedShift to simplify the encryption of your data within these services.

- AWS KMS enables you to create, rotate, disable, enable, and define usage policies for master keys and audit their usage.
- It is a centralized key management
- It is secure and compliant.

Why AWS Key Management Service?

Key Management Service is used to encrypt data in AWS. The main purpose of the AWS KMS is to store and manage those encryption keys. Data encryption is vital if you have sensitive data that must not be accessed by unauthorized users. Implement data encryption for both data at rest and data in transit.

Two main methods to implement encryption at rest are Client-Side Encryption and Server Side Encryption.

- **Client-Side Encryption is** where you can encrypt the data on the client side and send it all the way to the server or any backend services like S3, EBS, Redshift, etc. In short, we can say in client-side encryption you encrypt your data and manage your own keys.
- **Server-Side Encryption** AWS encrypts the data and manages the keys for you, whereas you let your backend services encrypt the data and manage those keys on your behalf.

Also read: This post covers the AWS Free Tier Account Overview. Amazon Web Services (AWS) is providing 12 months of Free Tier accounts to new subscribers to get hands-on experience with all the AWS cloud services.

Advantages of AWS KMS

1. **Fully Managed:** You access the encrypted data by assigning permissions to use the keys while AWS Key Management Service deals with the long-lasting and physical security of your keys, hence enforcing your permissions.
2. **Centralized Key Management:** AWS KMS provides a single point and defines policies continuously across AWS services and also your own applications. By using AWS CLI and SDK or AWS management console you can easily create, rotate, delete, and manage permissions on the keys.
3. **Manage Encryption for AWS Service:** AWS KMS is integrated with AWS services to simplify the encryption of data. KMS monitors the use of keys to AWS CloudTrail to give you a view of who accessed your encrypted data, including AWS services using them on your behalf.
4. **Encrypt Data In your Applications:** Using simple APIs you can also build encryption and key management into your own applications wherever they run. Using AWS SDK you can encrypt data locally within your application.
5. **Digitally Sign Data:** To maintain the integrity of your data, AWS Key Management Service enables you to perform digital signing using asymmetric key pairs.
6. **Low Cost:** As such there are no charges to use AWS Key Management Service. You are only charged when you use or manage the keys beyond the free tier.
7. **Secure:** AWS KMS uses hardware security modules that have been validated under FIPS 140-2(Federal Information Processing Standard Publication) or are in the process of being validated, to generate and protect keys. Your keys are only used inside these devices and can never leave them unencrypted. KMS keys are never shared outside the AWS region in which they were created.
8. **Compliance:** The security and quality controls in AWS KMS have been certified under multiple compliance schemes AWS KMS is also integrated with AWS CloudTrail for monitoring key usage so that your regulatory and compliance needs are met.