

Data Encryption

AWS Key Management Service (KMS)



Rajaram Erraguntla





REAL-TIME IT SOFTWARE EXAMPLE

Imagine you are developing a cloud-based collaboration platform for enterprises. This platform handles a vast amount of confidential data, including documents, messages, and user credentials.

To ensure the highest level of security, you can integrate AWS KMS into your software.





AWS KEY MANAGEMENT SERVICE (KMS)



KMS is a tool that helps keep your data safe in the cloud. It lets you create and manage special codes (keys) that protect your important information.

KMS also makes sure that only the right people can access your data.

5

PRE-REQUISITES

- 1. AWS Account** - We need an Active AWS Account.
- 2. IAM User or Role** : Ensure that you have the necessary access rights to work with KMS resources.
- 3. Basic AWS Knowledge** - Familiarity with concepts, such as IAM, AWS regions, and security best practices, is essential to use KMS effectively.
- 4. Encryption Requirements** - what data needs to be encrypted, the level of encryption required, and where the encrypted data will be used.
- 5. Security Best Practices** - Encryption is important to ensure the security of your data



STEP-BY-STEP PLAN TO CREATE KMS

- 1. Sign in to AWS Console**
- 2. Access the AWS KMS Service**
- 3. Create a New KMS Key**
- 4. Choose Key Creation Options**
- 5. Review and Confirm**
- 6. Key Creation Confirmation**

HANDS-ON

For a comprehensive hands-on guide on creating a Key Management Service (**KMS**), be sure to check out the blog linked in the **comments** section





WAS THIS

HELPFUL?



@iamrajaram1