# Project Overview

Amazon Key Management Service along with S3 and EBS data encryption

Amazon Web Services Key Management Service (KMS) is a managed service that simplifies the creation and management of encryption keys used to encrypt/decrypt your data. Most storage related AWS services are supported by KMS, including:

* 1. EBS (Elastic Block Store)
  2. S3 (Simple Storage Service)
  3. RDS (Relational Database Service)

This Project will include examples of encrypting EBS volumes and S3 buckets. It's important to understand that once setup is implemented, from a user's perspective the encryption of data is transparent. For example, if you look at a text file on an encrypted volume it is readable. That is because the encryption is not on a file by file basis, with some being encrypted and some that are not. Encryption takes place at a lower level (the operating system level). If you view a text file the decrypted file is displayed. Similarly, for S3 object storage... you can still view text files, images, etc. What volume encryption protects against is if someone gains physical access to the drive with the encrypted data on it. If they don't have the Customer Master Key (CMK) they cannot decrypt the contents.

# Project Architecture

