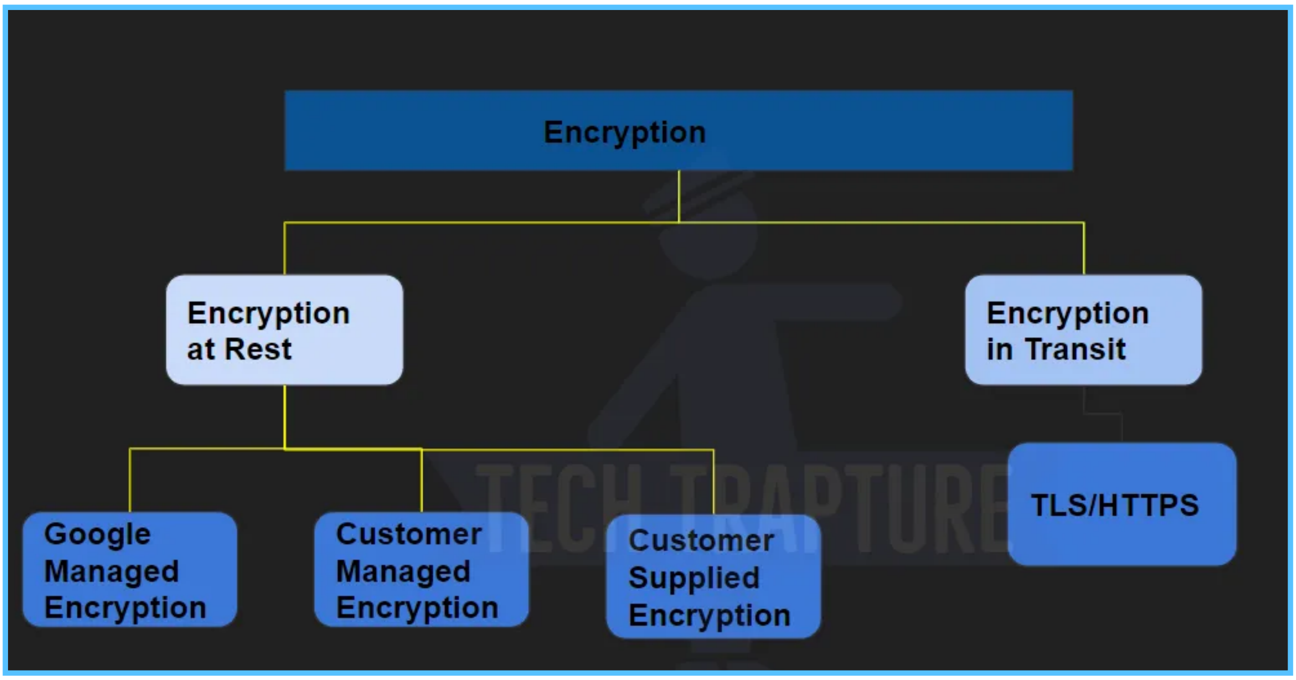
Overview on Types of Encryption in Google Cloud


Encryption
Encryption at Rest
Encryption in Transit
Google Managed Encryption
Customer Managed Encryption
Customer Supplied Encryption
TLS/HTTPS
TECH TRAPTURE

- *Encryption at rest is a security measure that protects data while it is stored on disk or in a database.*
- *It involves encrypting data before it is written to disk or database, so that if the data is accessed by an unauthorized user or attacker, they will not be able to read the sensitive information.*
- *Encryption at rest is particularly important for organizations that store sensitive data, such as personal information, financial records, or intellectual property.*
- *It can help protect against data breaches, theft, or unauthorized access.*

- *Encryption at rest is also often required to meet compliance standards, such as HIPAA, PCI DSS, or GDPR.*

Here are some of the encryption methods available for Data at rest :

- ***Google-managed encryption keys (GMEK):** All data that is stored by Google at rest is encrypted by default without any additional action using Google-managed keys, which are stored and managed by Google. There is no additional cost for Google-managed encryption keys.*
- ***Customer-managed encryption keys (CMEK):** This method allows customers to create and manage their own encryption keys in Google Cloud KMS, which are used to encrypt data at rest in Google Cloud Storage, Google BigQuery, Google Cloud SQL, and other services that support CMEK.*
- ***Customer-supplied encryption keys (CSEK):** This method allows customers to use their own encryption keys to encrypt data at rest in Google Cloud Storage and Google Compute disks. The keys are generated and managed by the customer, and are not stored in Google Cloud.*

Practical Implementation

Customer managed Encryption keys:

- *Create keyring in Cloud KMS*
- *Key will be managed by customer. Like Key rotation*

- *Key Management service â€“ GCP services*

Customer supplied Encryption keys - only in CLI commands

- *Want to supply own keys*
- *gsutil â€“ encrypt with CSEK*

o **Implementation**:

Generate Key with -- openssl rand -base64 32
ï‚§ (Csek-1)Copy the key
o Nano sample.txt (add some contents to it)
o Cat sample.txt
o gsutil ls â€“ list all the buckets in project
o gsutil cp sample.txt gs://(bucket-name)
ï‚§ Delete it bcoz its in google managed key
o mv sample.txt sample1.txt #rename file
o gsutil -o â€˜GSUtil:encryption_key=(Csek-1)â€™ cp sample1.txt gs://(bucket-name)

o **To view it:**

- *ï‚§ gsutil -o â€˜GSUtil:encryption_key=(Csek-1)â€™ cat gs://(bucket-name)/sample1.txt*