

# Create an S3 bucket with versioning enabled for the objects. Map out a bucket policy such that every object we put within the bucket needs to be encrypted by default using KMS keys: -

## 1: - Created a Bucket with Versioning: -

Successfully created bucket "itt-bucket"  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Amazon S3 > Buckets

**Account snapshot** [View Storage Lens dashboard](#)  
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

General purpose buckets | Directory buckets

**General purpose buckets (1)** [Info](#)  
Buckets are containers for data stored in S3. [Learn more](#)

< 1 > [Settings](#)

Name	AWS Region	Access	Creation date
<input type="radio"/> itt-bucket	Asia Pacific (Mumbai) ap-south-1	<a href="#">Bucket and objects not public</a>	February 3, 2024, 21:39:04 (UTC+05:30)

## 2: - Created a KMS Key: -

aws Services Search [Alt+S] Mumbai MIHIR JAIN

**Key Management Service (KMS)**

AWS managed keys  
Customer-managed keys

▼ Custom key stores  
AWS CloudHSM key stores  
External key stores

KMS > Customer-managed keys

**Customer-managed keys (2)** [Key actions](#) [Create key](#)

< 1 > [Settings](#)

<input type="checkbox"/>	Aliases	Key ID	Status	Key type	Key spec	Key usage
<input type="checkbox"/>	<a href="#">bucket-key</a>	bfb37a7-492...	Pending deletion	Symmetric	SYMMETRIC_D...	Encrypt and de...
<input type="checkbox"/>	<a href="#">Itt-Bucket-key</a>	dba7120a-3b0...	Enabled	Symmetric	SYMMETRIC_D...	Encrypt and de...

- Created symmetric key in this key
- Name of the key is Itt-bucket-key
- Created a KMS Key with only key administrator can access the key
- After that key users cannot access the key that I am selected

### 3: - Bucket versioning is enabled: -

**Amazon S3**

**Buckets**

- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

▼ **Storage Lens**

- Dashboards
- Storage Lens groups
- AWS Organizations settings

**Properties** | Permissions | Metrics | Management | Access Points

**Bucket overview**

AWS Region Asia Pacific (Mumbai) ap-south-1	Amazon Resource Name (ARN) arn:aws:s3:::itt-bucket	Creation date February 3, 2024, 22:23:14 (UTC+05:30)
--	---	---

**Bucket Versioning** Edit

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning  
Enabled  
Multi-factor authentication (MFA) delete  
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)  
Disabled

### 4: - In the Bucket We added an Encryption Key: -

**Amazon S3**

**Buckets**

- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

▼ **Storage Lens**

- Dashboards
- Storage Lens groups
- AWS Organizations settings

**Properties** | Permissions | Metrics | Management | Access Points

**Key** | Value

No tags associated with this resource.

**Default encryption** Info Edit

Server-side encryption is automatically applied to new objects stored in this bucket.

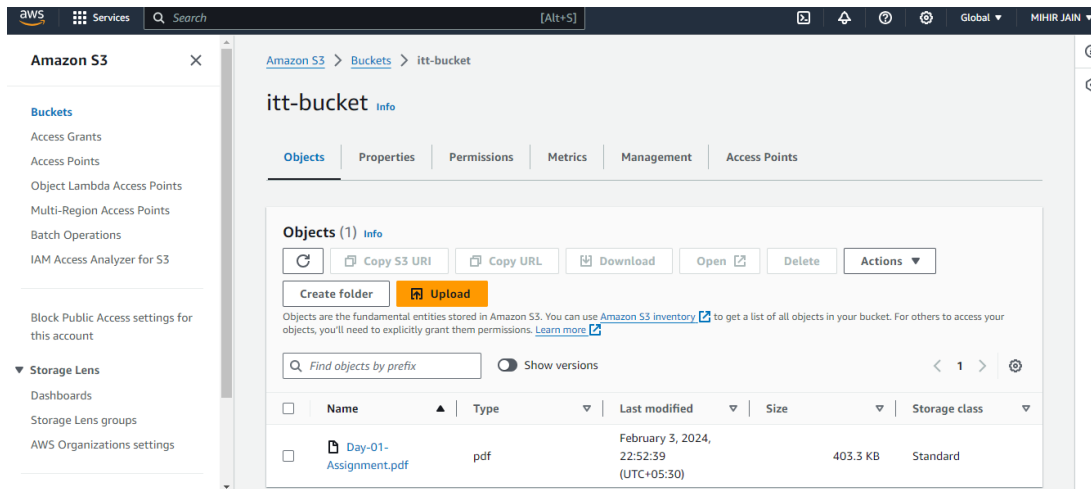
Encryption type Info  
Server-side encryption with AWS Key Management Service keys (SSE-KMS)

Encryption key ARN  
arn:aws:kms:ap-south-1:975050349146:key/dba7120a-3b02-4533-940c-f793b262a89d

Bucket Key  
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)  
Enabled

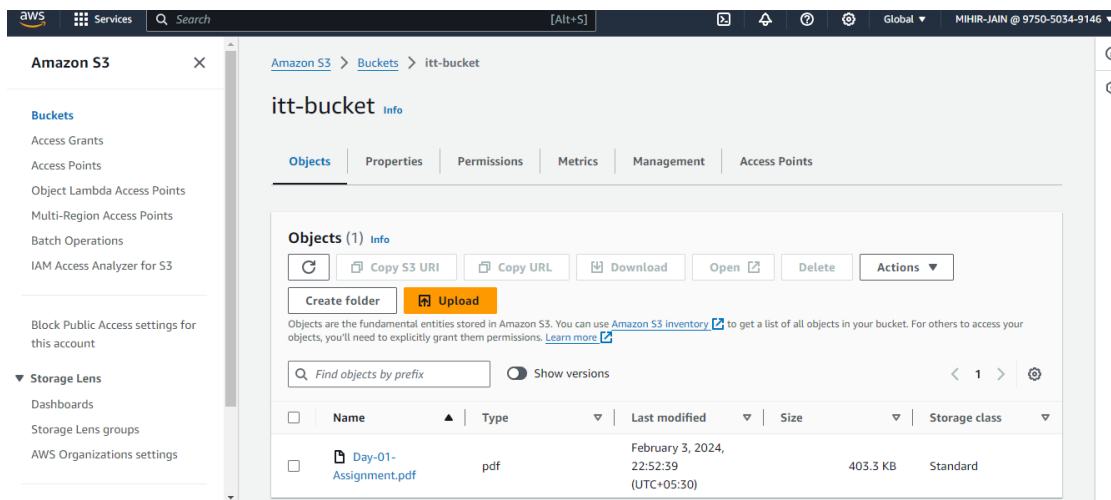
**Intelligent-Tiering Archive configurations (0)**

## 5: - After That I uploaded one file in this bucket from the root user: -

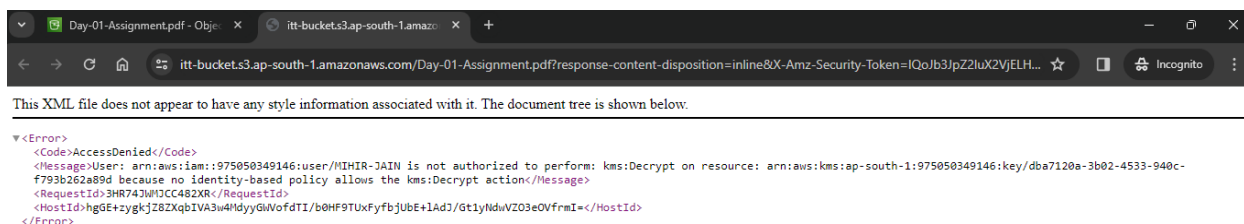


- I am giving IAM policy to user to full access of s3 bucket

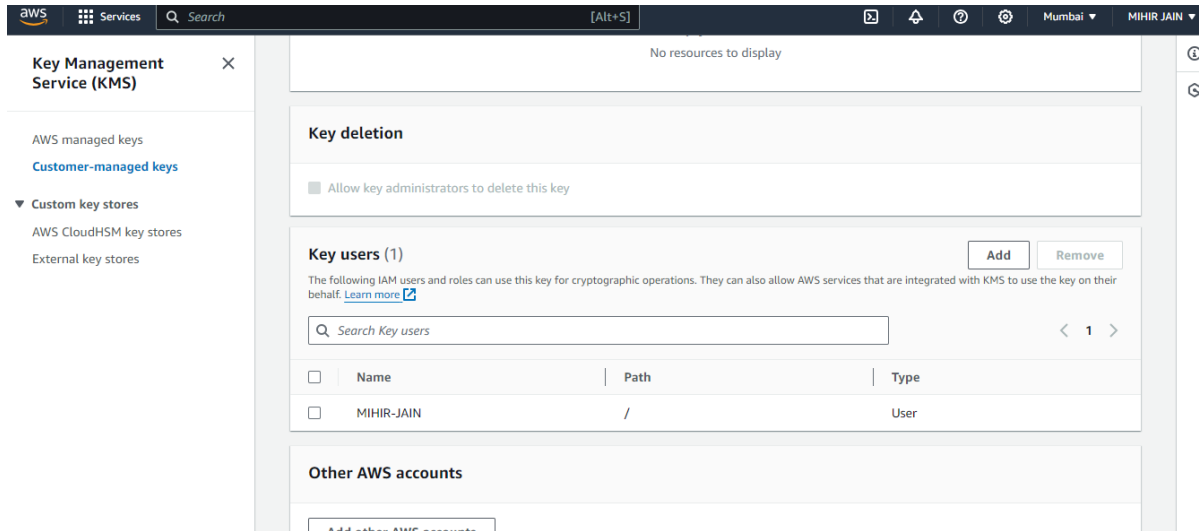
## 6: - Login From The user and check the file inside the bucket that root user is uploaded:-



- So, the user can see the file that root user is uploaded but user have no access to see the file or upload a file in the bucket because the bucket is encrypted by the KMS key.



## 6: - So, I am added the user to access the ITT-bucket files: -



- The user can view the file after I added in the key users of the key management service.
- Users have full access to the uploading and editing in the files of bucket.