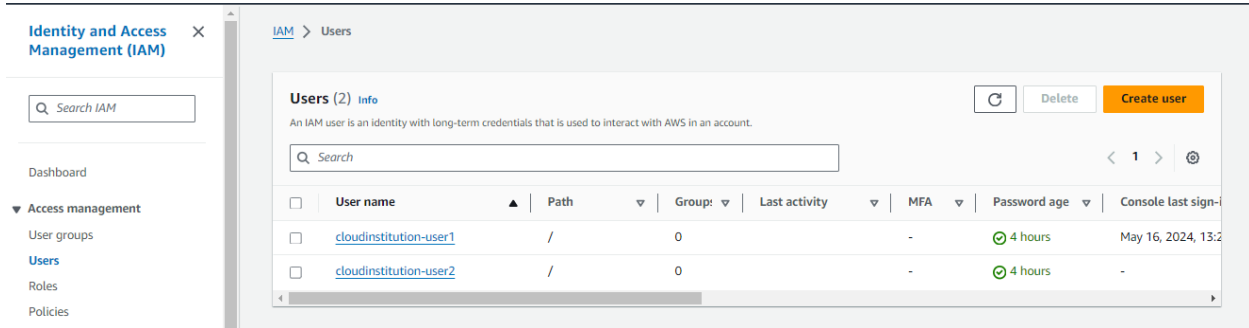


S3 OBJECT ENCRYPTION AND DECRYPTION BY USING KMS

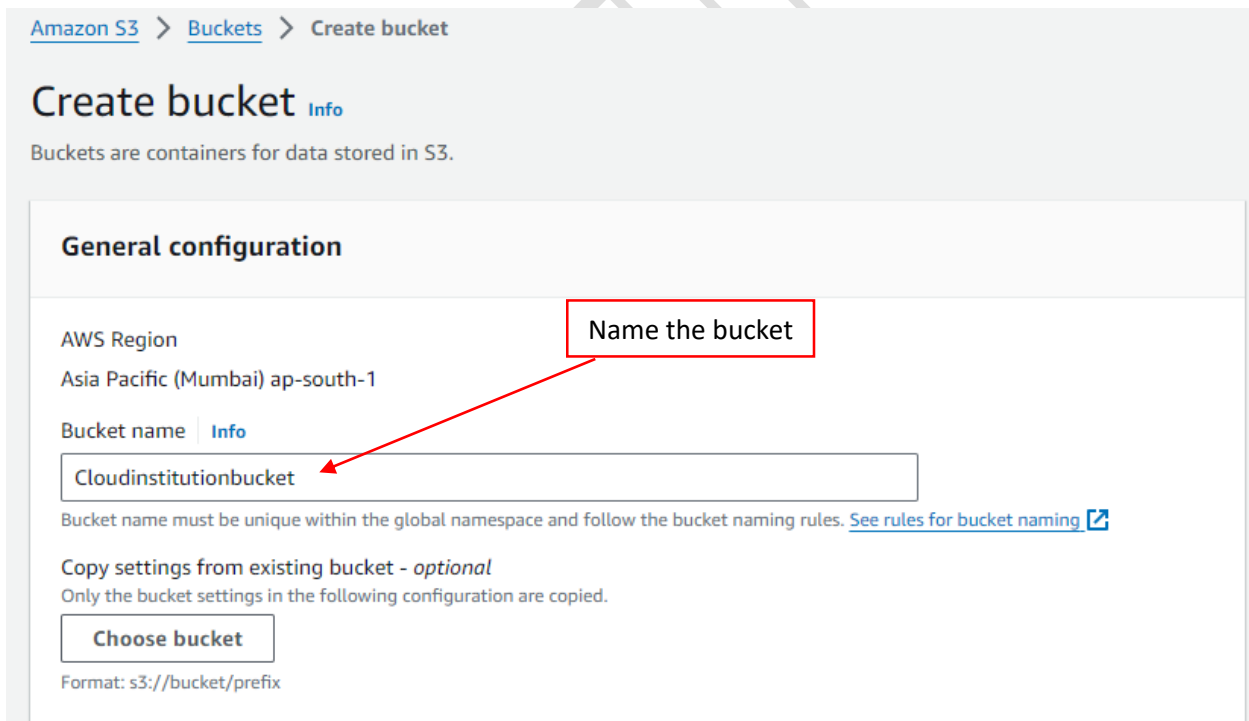
Step 1 : Create 2 IAM Users with permission policy - S3 full access



The screenshot shows the AWS IAM console 'Users' page. On the left, the 'Identity and Access Management (IAM)' sidebar is visible with a search bar and navigation links for Dashboard, Access management, User groups, Users, Roles, and Policies. The main content area shows 'Users (2)' with a search bar and a table of users. The table has columns for checkboxes, User name, Path, Group, Last activity, MFA, Password age, and Console last sign-in. Two users are listed: 'cloudinstitution-user1' and 'cloudinstitution-user2', both with a path of '/', group of '0', and password age of '4 hours'.

	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
<input type="checkbox"/>	cloudinstitution-user1	/	0		-	4 hours	May 16, 2024, 13:2
<input type="checkbox"/>	cloudinstitution-user2	/	0		-	4 hours	-

Step 2 : Create a bucket



The screenshot shows the 'Create bucket' page in the AWS S3 console. The breadcrumb navigation is 'Amazon S3 > Buckets > Create bucket'. The page title is 'Create bucket' with an 'Info' link. Below the title, it says 'Buckets are containers for data stored in S3.' The 'General configuration' section is expanded, showing 'AWS Region' as 'Asia Pacific (Mumbai) ap-south-1'. The 'Bucket name' field is highlighted with a red box and labeled 'Name the bucket' with a red arrow. The bucket name entered is 'Cloudinstitutionbucket'. Below the field, a note states: 'Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming'. There is a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. At the bottom, the format 'Format: s3://bucket/prefix' is shown.

Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ **ACLs disabled (recommended)**

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☐ **ACLs enabled**

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ **Block all public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☒ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☒ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**

S3 will ignore all ACLs that grant public access to buckets and objects.

☒ **Block public access to buckets and objects granted through *new* public bucket or access point policies**

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☒ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Default encryption [Info](#)

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

Choose SSE-KMS

Encryption type [Info](#)

- ☐ Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ☒ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the **Storage** tab of the [Amazon S3 pricing page](#).

AWS KMS key [Info](#)

- ☒ Choose from your AWS KMS keys
- ☐ Enter AWS KMS key ARN

Click on create

Available AWS KMS keys

Choose AWS KMS key



Create a KMS key [↗](#)

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- ☐ Disable
- ☒ Enable

Step 3 : Create a KMS key

Step 2
Add labels

Step 3
Define key administrative
permissions

Step 4
Define key usage permissions

Step 5
Review

Key type [Help me choose](#)

☒ Symmetric

A single key used for encrypting and decrypting data or generating and verifying HMAC codes

☐ Asymmetric

A public and private key pair used for encrypting and decrypting data or signing and verifying messages

Key usage [Help me choose](#)

☒ Encrypt and decrypt

Use the key only to encrypt and decrypt data.

☐ Generate and verify MAC

Use the key only to generate and verify hash-based message authentication codes (HMAC).

► Advanced options

Click advanced options

Cancel

Next

▼ Advanced options

Choose recommended KMS

Key material origin

Key material origin is a KMS key property that represents the source of the key material when creating the KMS key. [Help me choose](#)

☒ **KMS - recommended**

AWS KMS creates and manages the key material for the KMS key.

☐ **External (Import Key material)**

You create and import the key material for the KMS key.

☐ **AWS CloudHSM key store**

AWS KMS creates the key material in the AWS CloudHSM cluster of your AWS CloudHSM key store.

☐ **External key store**

The key material for the KMS key is in an external key manager outside of AWS.

Regionality

Create your KMS key in a single AWS Region (default) or create a KMS key that you can replicate into multiple AWS Regions. [Help me choose](#)

☒ **Single-Region key**

Never allow this key to be replicated into other Regions

☐ **Multi-Region key**

Allow this key to be replicated into other Regions

Click next

Cancel

Next

KMS > [Customer managed keys](#) > Create key

Step 1

[Configure key](#)

Step 2

Add labels

Step 3

Define key administrative permissions

Step 4

Define key usage permissions

Step 5

Review

Add labels

Alias

You can change the alias at any time. [Learn more](#)

Alias

Cloudinstitutionkmskey

Give a name to the KMS key

Description - optional

You can change the description at any time.

Description

Description of the key

Step 2
[Add labels](#)

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review

Key administrators (4)

Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. [Learn more](#)

Search Key administrators

<input type="checkbox"/>	Name	Path	Type
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling...	Role
<input type="checkbox"/>	AWSServiceRoleForElasticLoa...	/aws-service-role/elasticloadb...	Role
<input type="checkbox"/>	AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
<input type="checkbox"/>	AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role

Key deletion

☒ Allow key administrators to delete this key.

Click next

Cancel Previous Next

Here I'm giving access only to user1

Key users (1/6)

Select the IAM users and roles that can use the KMS key in cryptographic operations. [Learn more](#)

Search Key users

Select user1

<input type="checkbox"/>	Name	Path	Type
<input checked="" type="checkbox"/>	cloudinstitution-user1	/	User
<input type="checkbox"/>	cloudinstitution-user2	/	User
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling...	Role
<input type="checkbox"/>	AWSServiceRoleForElasticLoa...	/aws-service-role/elasticloadb...	Role
<input type="checkbox"/>	AWSServiceRoleForSupport	/aws-service-role/support.am...	Role
<input type="checkbox"/>	AWSServiceRoleForTrustedAd...	/aws-service-role/trustedadvis...	Role

Other AWS accounts

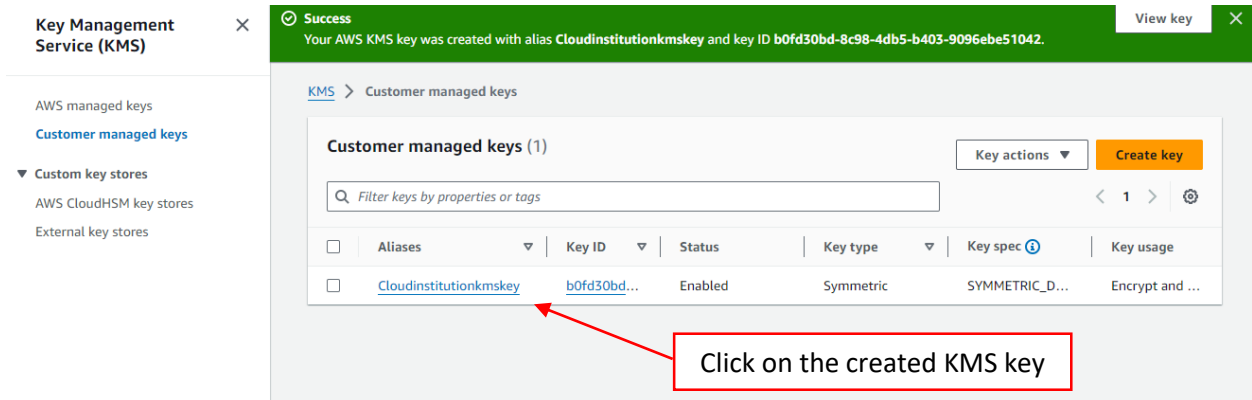
Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

Add another AWS account

Click next

Cancel Previous Next

Review and click Finish



Key Management Service (KMS)

Success
Your AWS KMS key was created with alias **Cloudinstitutionkmskey** and key ID **b0fd30bd-8c98-4db5-b403-9096ebe51042**.

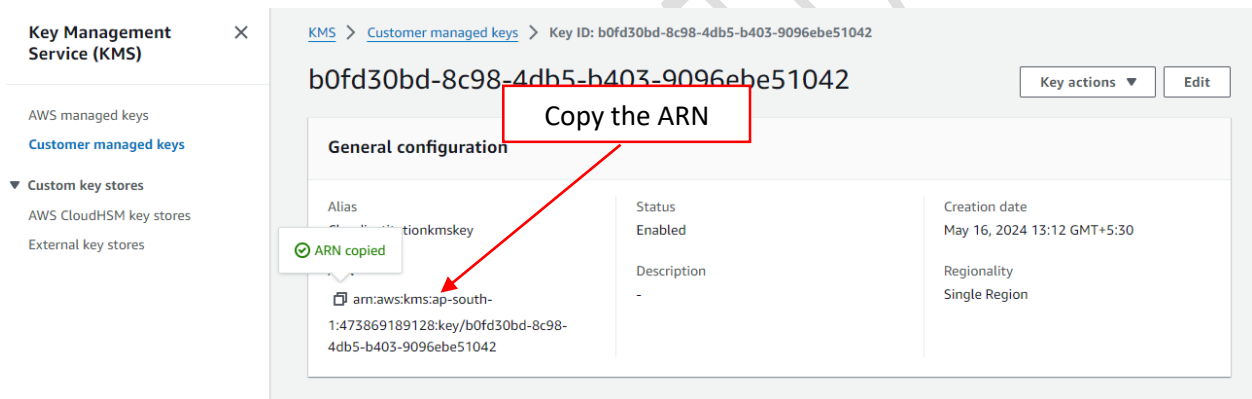
KMS > Customer managed keys

Customer managed keys (1)

Filter keys by properties or tags

	Aliases	Key ID	Status	Key type	Key spec	Key usage
<input type="checkbox"/>	Cloudinstitutionkmskey	b0fd30bd...	Enabled	Symmetric	SYMMETRIC_D...	Encrypt and ...

Click on the created KMS key



Key Management Service (KMS)

KMS > Customer managed keys > Key ID: b0fd30bd-8c98-4db5-b403-9096ebe51042

b0fd30bd-8c98-4db5-b403-9096ebe51042

Key actions Edit

General configuration

Alias Cloudinstitutionkmskey	Status Enabled	Creation date May 16, 2024 13:12 GMT+5:30
arn:aws:kms:ap-south-1:473869189128:key/b0fd30bd-8c98-4db5-b403-9096ebe51042	Description -	Regionality Single Region

Copy the ARN

Now go back to the S3 bucket creation page

Default encryption

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

Encryption type [Info](#)

- ☐ Server-side encryption with Amazon S3 managed keys (SSE-S3)
- ☒ Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- ☐ Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the **Storage** tab of the [Amazon S3 pricing page](#). [↗](#)

AWS KMS key [Info](#)

- ☐ Choose from your AWS KMS keys
- ☒ Enter AWS KMS key ARN

AWS KMS key ARN

[Create a KMS key](#) [↗](#)

Format (using key id): `arn:aws:kms:<region>:<account-ID>:key/<key-id>`
(using alias): `arn:aws:kms:<region>:<account-ID>:alias/<alias-name>`

Paste the copied ARN

Bucket Key

Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#) [↗](#)

- ☐ Disable
- ☒ Enable

► Advanced settings

Click create

[i](#) After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

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

Successfully created bucket "cloudinstitutionbucket"
To upload files and folders, or to configure additional bucket settings, choose View details.

General purpose buckets | Directory buckets

General purpose buckets (1) Info All AWS Regions

Copy ARN Empty Delete Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

Bucket created

Name	AWS Region	IAM Access Analyzer	Created
cloudinstitutionbucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	May 2024 13:00 (UTC)

Step 4 : Upload a file to the bucket

cloudinstitutionbucket Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (2) Info

Copy S3 URI Copy URL Download Open Delete Actions Create folder

Upload

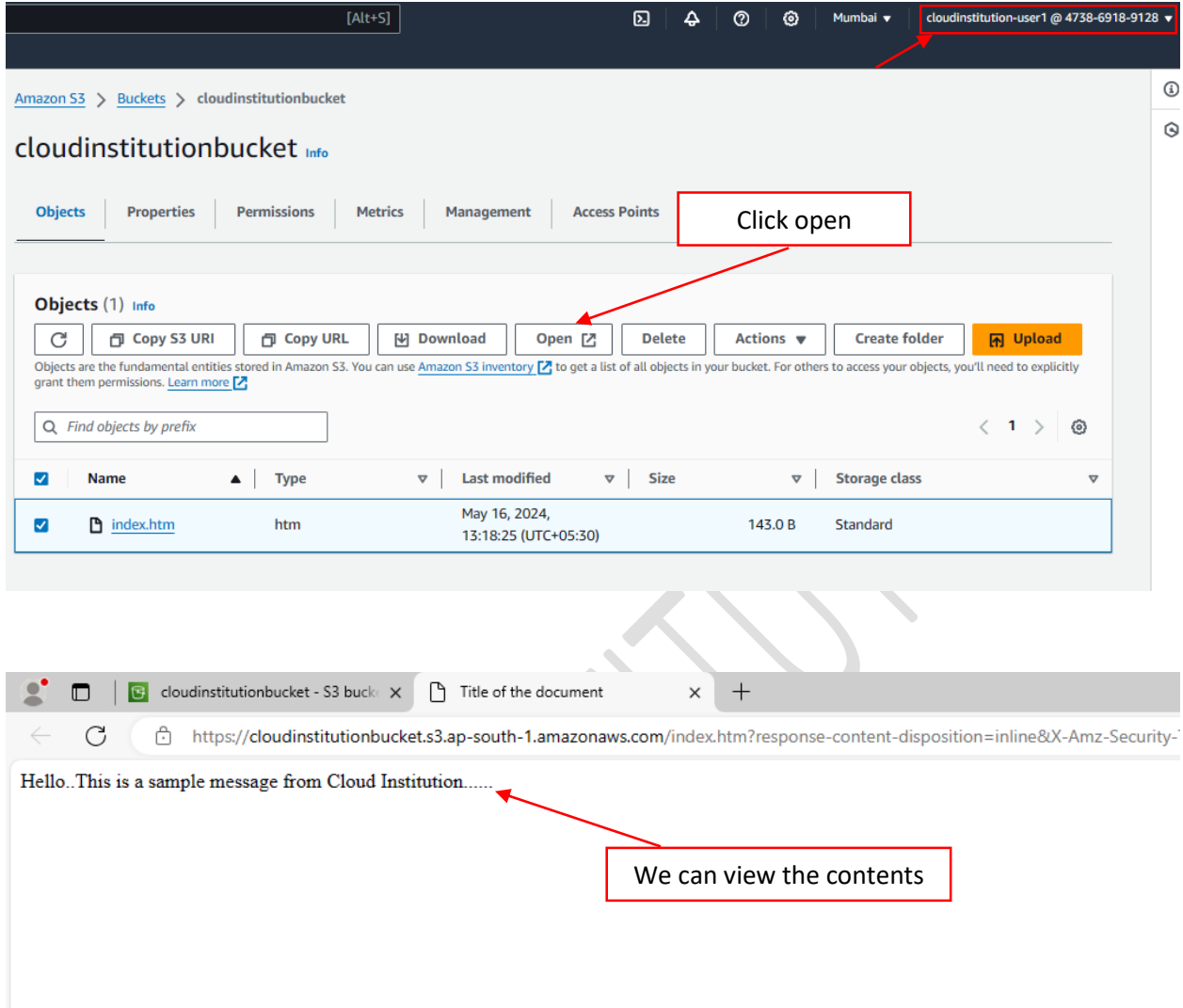
Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

File uploaded

Name	Type	Last modified	Size	Storage class
index.htm	htm	May 16, 2024, 16:25:41 (UTC+05:30)	170.0 B	Standard

Step 5 : Now login to the IAM user – cloudinstitution-user1



[Alt+S] Mumbai cloudinstitution-user1 @ 4738-6918-9128

Amazon S3 > Buckets > cloudinstitutionbucket

cloudinstitutionbucket [Info](#)

[Objects](#) | [Properties](#) | [Permissions](#) | [Metrics](#) | [Management](#) | [Access Points](#) **Click open**

Objects (1) [Info](#)

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

<input checked="" type="checkbox"/>	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	index.htm	htm	May 16, 2024, 13:18:25 (UTC+05:30)	143.0 B	Standard

cloudinstitutionbucket - S3 bucket x Title of the document x +

https://cloudinstitutionbucket.s3.ap-south-1.amazonaws.com/index.htm?response-content-disposition=inline&X-Amz-Security-

Hello.. This is a sample message from Cloud Institution..... **We can view the contents**

Step 6 : Now login to the IAM user – cloudinstitution-user2

[Alt+S] Mumbai cloudinstitution-user2 @ 4738-6918-9128

Amazon S3 > Buckets > cloudinstitutionbucket

cloudinstitutionbucket [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Click open

Objects (2) [Info](#)

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#) [Upload](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

	Name	Type	Last modified	Size	Storage class
<input checked="" type="checkbox"/>	index.htm	htm	May 16, 2024, 16:25:41 (UTC+05:30)	170.0 B	Standard

Access is denied because we did not give access to the user2

cloudinstitutionbucket - S3 bucket cloudinstitutionbuckets3.ap-sou...
https://cloudinstitutionbuckets3.ap-south-1.amazonaws.com/cloud.htm?response-content-disposition=inline&X-Amz-Security-Token=IQ...

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<Error>
  <Code>AccessDenied</Code>
  <Message>User: arn:aws:iam::473869189128:user/cloudinstitution-user2 is not authorized to perform: kms:Decrypt on resource: arn:aws:kms:ap-south-1:473869189128:key/cd9b370b-b8f6-453e-8e55-772717240641 because no identity-based policy allows the kms:Decrypt action</Message>
  <RequestId>QPKCP2MMYGZRGJDD</RequestId>
  <HostId>ogHs/4DzUK5Z1+zBPqo4HA88/ONCs2nOkmL7NpXL/SHqnO+vm32ZZzELdk2FxsHrAE0QN8rXhN0=</HostId>
</Error>
```