



School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 9. Implementing S3 Encryption with AWS KMS and Activity Monitoring via CloudTrail.

Step 1: Create one S3 Bucket.

- Go to S3 in AWS Dashboard.
- Click on Create bucket.
- Select Bucket type as "General Purpose".
- Give proper name to bucket as 'bucket-lab9-2265'.

Create bucket [Info](#)

Buckets are containers for data stored in S3.

General configuration

AWS Region

Asia Pacific (Mumbai) ap-south-1

Bucket type [Info](#)



General purpose

Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.

Bucket name [Info](#)

bucket-lab9-2265

Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

- In "Object Ownership" click on "ACLs enabled".
- In "Object Ownership" select "Object writer".
- Block all Public Access and then click Create Bucket.

School of Computer Science, Engineering and Applications (SCSEA)
B. Tech TY (CCSA)
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade **PRN: 20220802265**

Title of Practical: 9. Implementing S3 Encryption with AWS KMS and Activity Monitoring via CloudTrail.

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.

⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

Object Ownership

☐ **Bucket owner preferred**
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☒ **Object writer**
The object writer remains the object owner.

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.

Step 2: In CloudTrail create one Trail.

- Go to CloudTrail in AWS Dashboard.
- Click on Create Trail.
- Give proper name to trail as 'CldTrail-2265'.
- Select our existing Bucket i.e. – bucket-lab9-2265.
- Enable “Log file SSE-KMS encryption”.

Step 1
Choose trail attributes

General details
A trail created in the console is a multi-region trail. [Learn more](#)

Trail name
Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

☐ **Enable for all accounts in my organization**
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

Storage location [Info](#)

☐ **Create new S3 bucket**
Create a bucket to store logs for the trail.

☒ **Use existing S3 bucket**
Choose an existing bucket to store logs for this trail.

Trail log bucket name
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.
 [Browse](#)

Prefix - optional

Logs will be stored in bucket-lab9-2265/AWSLogs/908027405956

Log file SSE-KMS encryption [Info](#)
☒ **Enabled**

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

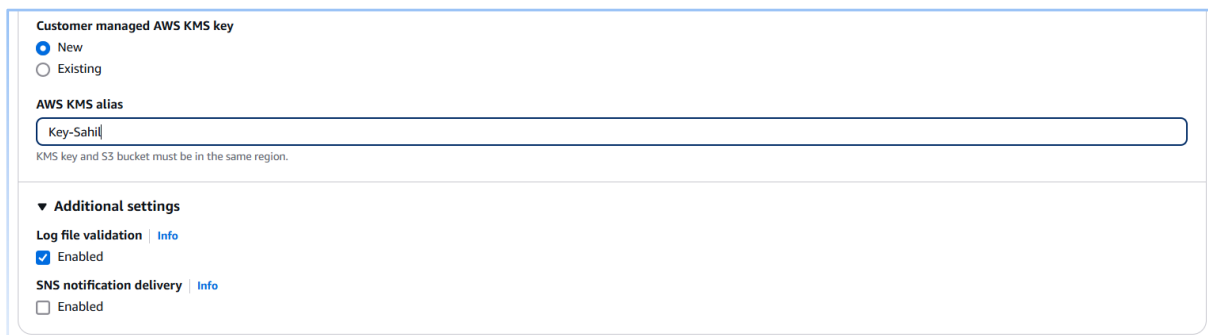
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

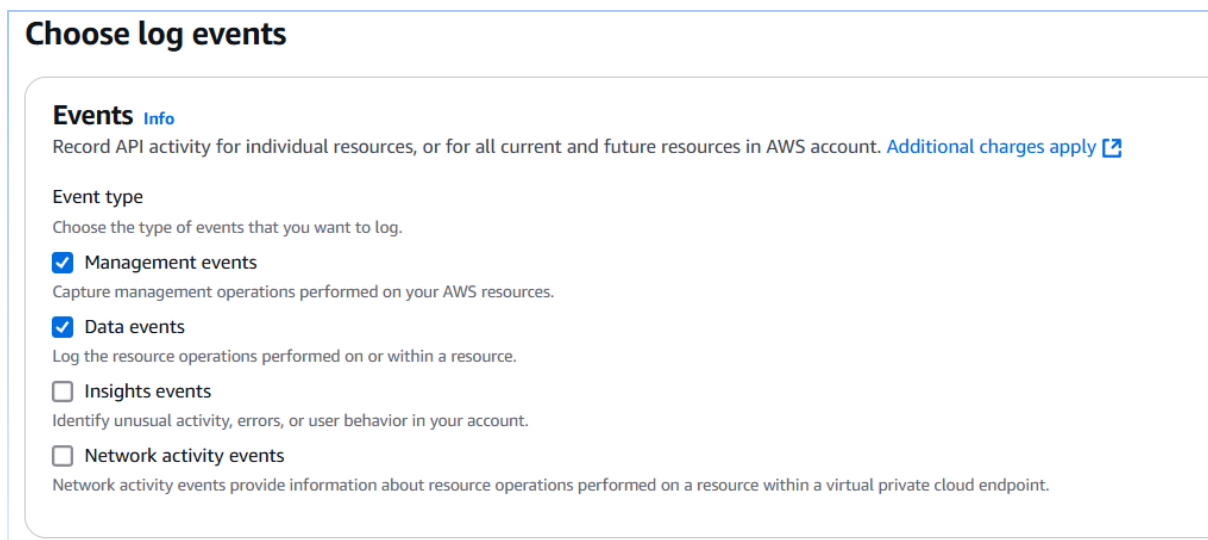
Title of Practical: 9. Implementing S3 Encryption with AWS KMS and Activity Monitoring via CloudTrail.

- Select “New” in Customer managed AWS KMS keys.
- Give proper key alias.
- Enable “Log file validation”.



The screenshot shows the 'Create new key' page in the AWS KMS console. Under 'Customer managed AWS KMS key', the 'New' radio button is selected. The 'AWS KMS alias' text box contains 'Key-Sahil'. Below this, a note states 'KMS key and S3 bucket must be in the same region.' Under the 'Additional settings' section, 'Log file validation' is checked and labeled 'Enabled', and 'SNS notification delivery' is unchecked.

- In Events click on “Management” & “Data” events.



The screenshot shows the 'Choose log events' page in the AWS CloudTrail console. Under the 'Events' section, 'Management events' and 'Data events' are both checked. Descriptions for each event type are provided. 'Insights events' and 'Network activity events' are unchecked.

- In Management Event Select “Read” & “Write”.

School of Computer Science, Engineering and Applications (SCSEA)

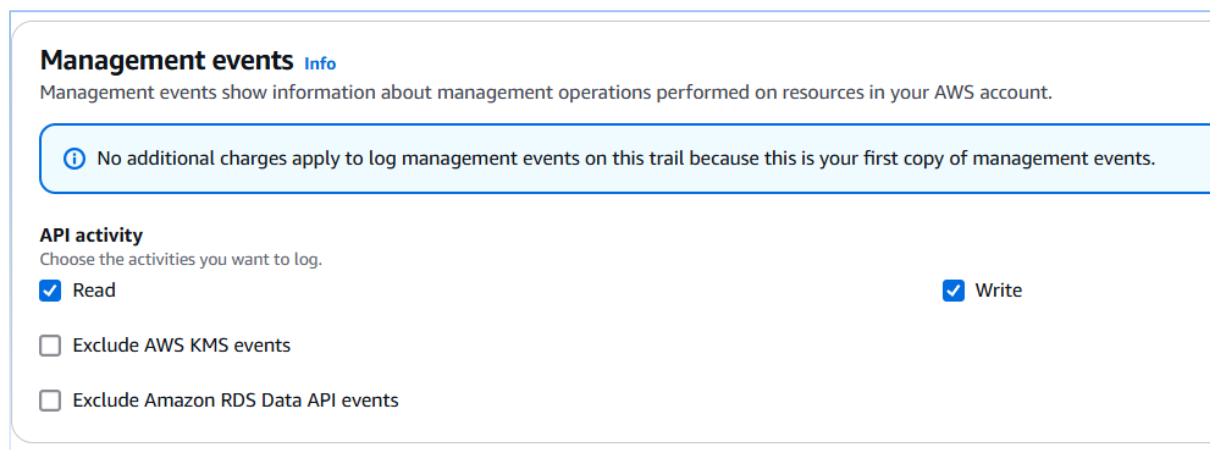
B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 9. Implementing S3 Encryption with AWS KMS and Activity Monitoring via CloudTrail.



Management events [Info](#)
Management events show information about management operations performed on resources in your AWS account.

No additional charges apply to log management events on this trail because this is your first copy of management events.

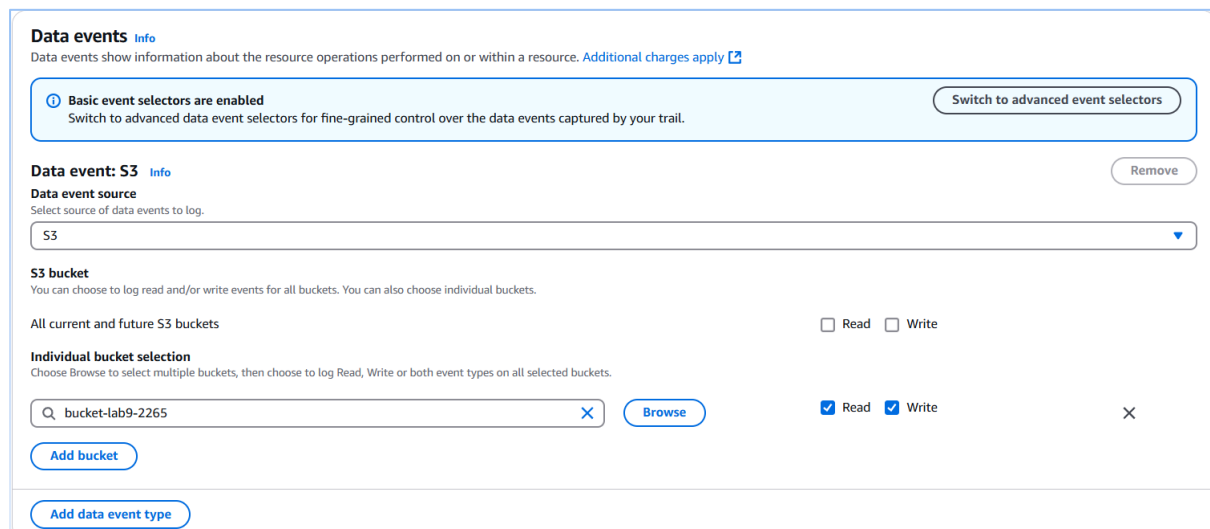
API activity
Choose the activities you want to log.

☒ Read ☒ Write

☐ Exclude AWS KMS events

☐ Exclude Amazon RDS Data API events

- In Data Event : Switch to basic event selectors – Select “Read” & “Write” on our created bucket.



Data events [Info](#)
Data events show information about the resource operations performed on or within a resource. [Additional charges apply](#)

Basic event selectors are enabled
Switch to advanced data event selectors for fine-grained control over the data events captured by your trail. [Switch to advanced event selectors](#)

Data event: S3 [Info](#) [Remove](#)

Data event source
Select source of data events to log.
S3

S3 bucket
You can choose to log read and/or write events for all buckets. You can also choose individual buckets.

All current and future S3 buckets ☐ Read ☐ Write

Individual bucket selection
Choose Browse to select multiple buckets, then choose to log Read, Write or both event types on all selected buckets.

Q bucket-lab9-2265 X [Browse](#) ☒ Read ☒ Write X

[Add bucket](#)

[Add data event type](#)

- Review all the settings and Create the Trail.

Step 3: Upload file in S3 bucket with encryption.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

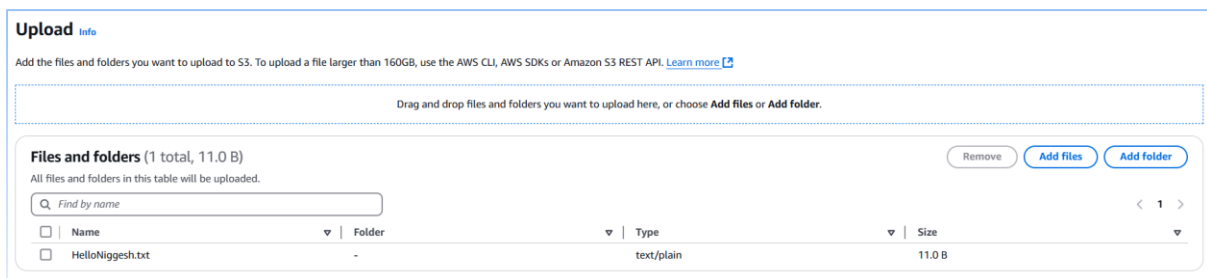
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 9. Implementing S3 Encryption with AWS KMS and Activity Monitoring via CloudTrail.

- Select our created bucket and click on “upload”.
- Add one file in bucket.



Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

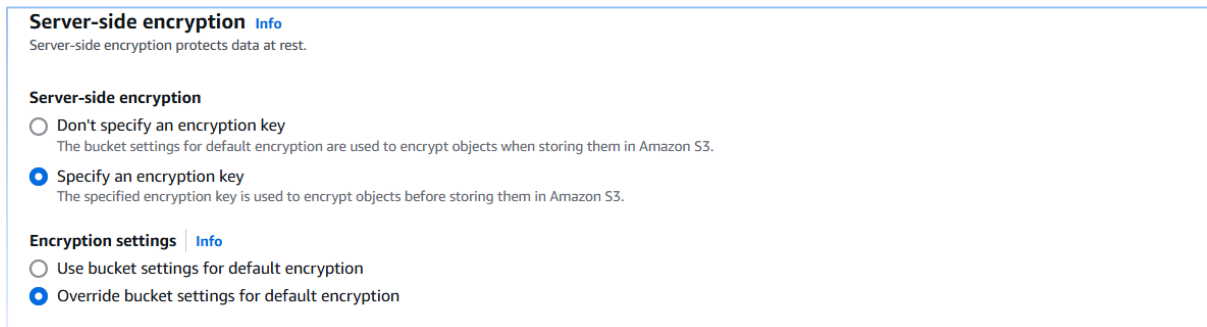
Files and folders (1 total, 11.0 B)

All files and folders in this table will be uploaded.

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	HelloNiggesh.txt	-	text/plain	11.0 B

[Remove](#) [Add files](#) [Add folder](#)

- Go in properties and in “server-side encryption” select “specify an encryption key”.



Server-side encryption [Info](#)

Server-side encryption protects data at rest.

Server-side encryption

☐ Don't specify an encryption key
The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.

☒ Specify an encryption key
The specified encryption key is used to encrypt objects before storing them in Amazon S3.

Encryption settings | [Info](#)

☐ Use bucket settings for default encryption

☒ Override bucket settings for default encryption

- In “Encryption Type” select “Server-side encryption with AWS Key Management Service (SSE-KMS)”.
- In AWS KMS Key select our created key.

School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 9. Implementing S3 Encryption with AWS KMS and Activity Monitoring via CloudTrail.

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

Available AWS KMS keys

[↻](#) [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 4: Check if our key is used for Encryption using Key ID.

- Go to KMS and copy the Key ID.

d0a4851f-c4fc-4c82-a0e6-1681331a9a24 [←](#) [Key actions](#) [Edit](#)

General configuration

Alias Key-Sahil	Status Enabled	Creation date Apr 03, 2025 02:17 GMT+5:30
ARN  arn:aws:kms:ap-south-1:908027405956:key/d0a4851f-c4fc-4c82-a0e6-1681331a9a24	Description -	Regionality Single Region

- Now in S3 click on our bucket.
- In Bucket go in following Path:

[Amazon S3](#) > [Buckets](#) > [bucket-lab9-2265](#) > [AWSLogs/](#) > [908027405956/](#) > [CloudTrail/](#) > [ap-south-1/](#) > [2025/](#) > [04/](#) > [02/](#) > [908027405956_CloudTrail_ap-sout...](#)

- Open the logs -> Ctrl+f.
- Paste our key ID and see if it's used.



School of Computer Science, Engineering and Applications (SCSEA)

B. Tech TY (CCSA)

Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade

PRN: 20220802265

Title of Practical: 9. Implementing S3 Encryption with AWS KMS and Activity Monitoring via CloudTrail.

```
https://bucket-lab9-2265.s3.ap-south-1.amazonaws.com/AWSLogs/908027405956/CloudTrail/ap-south-1/2025/04/02/908027405956_CloudTrail_ap-south-1_20250402T100...
Pretty-print
{"Records":[{"eventVersion":"1.11","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2025-04-02T20:52:17Z","eventSource":"kms.amazonaws.com","eventName":"GenerateDataKey","awsRegion":"ap-south-1","sourceIPAddress":"cloudtrail.amazonaws.com","userAgent":"cloudtrail.amazonaws.com","requestParameters":{"keyId":"arn:aws:kms:ap-south-1:908027405956:key/d0a4851f-c4fc-4c82-a0e6-1681331a9a24","encryptionContext":{"aws:cloudtrail:arn":"arn:aws:cloudtrail:ap-south-1:908027405956:trail/CloudTrail-2265","aws:s3:arn":"arn:aws:s3:::bucket-lab9-2265"},"keySpec":"AES_256"},"responseElements":null,"requestID":"24d1feba-591a-403d-8a9e-f71a4c63bc6f","eventID":"31b3e532-d365-349e-b8f9-6ea5f38078c4","readOnly":true,"resources":[{"accountId":"908027405956","type":"AWS::KMS::Key","ARN":"arn:aws:kms:ap-south-1:908027405956:key/d0a4851f-c4fc-4c82-a0e6-1681331a9a24"}],"eventCategory":"Management","eventVersion":"1.11","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2025-04-02T20:52:15Z","eventSource":"s3.amazonaws.com","eventName":"GetBucketAcl","awsRegion":"ap-south-1","sourceIPAddress":"cloudtrail.amazonaws.com","userAgent":"cloudtrail.amazonaws.com","requestParameters":{"bucketName":"bucket-lab9-2265.s3.ap-south-1.amazonaws.com","acl":"","responseElements":null,"additionalEventData":{"SignatureVersion":"SigV4","CipherSuite":"TLS_AES_128_GCM_SHA256","bytesTransferredIn":0,"AuthenticationMethod":"AuthHeader","x-amz-id-2":"Qso61zXg4H78LVfoejJHKnF20KmFWTnZE59mB0nbSbKgyGLRBBagXV7cCp14wkq1kXSM9eaAHsg6aUkrxwCqQ==","bytesTransferredOut":480},"requestID":"DZ7CFF4X5G1WAGM4","eventID":"af4d67-79-2d34-3c87-a78d-ccf76ad32b87","readOnly":true,"resources":[{"accountId":"908027405956","type":"AWS::S3::Bucket","ARN":"arn:aws:s3:::bucket-lab9-2265"}],"eventCategory":"Management","eventVersion":"1.11","userIdentity":{"type":"AWSService","invokedBy":"cloudtrail.amazonaws.com"},"eventTime":"2025-04-02T20:53:38Z","eventSource":"s3.amazonaws.com","eventName":"GetBucketAcl","awsRegion":"ap-south-1","sourceIPAddress":"cloudtrail.amazonaws.com","userAgent":"cloudtrail.amazonaws.com","requestParameters":{"bucketName":"bucket-lab9-2265.s3.ap-south-1.amazonaws.com","acl":"","responseElements":null,"additionalEventData":{"SignatureVersion":"SigV4","CipherSuite":"TLS_AES_128_GCM_SHA256","bytesTransferredIn":0,"AuthenticationMethod":"AuthHeader","x-amz-id-2":"3seVxHsEj4y/VLEa3xks+mmCmyZ9yJqZJ2hPG80WgARarNZDCVY6trCz/H4jUyL49q8BR5GEWw=","bytesTransferredOut":480},"requestID":"MAMNWD9W43SV2XDS","eventID":"a96c1c0c-332f-3aca-9fa3-907616891cc7","readOnly":true,"resources":[{"accountId":"908027405956","type":"AWS::S3::Bucket","ARN":"arn:aws:s3:::bucket-lab9-2265"}],"eventCategory":"Management","eventVersion":"1.11","userIdentity":{"type":"Root","principalId":"908027405956","arn":"arn:aws:iam:908027405956:root","accountId":"908027405956","accessKeyId":"ASIA5G2VGU2CAR750BJA","userName":"sahil021","sessionContext":{"attributes":{"creationDate":"2025-04-02T18:01:56Z","mfaAuthenticated":"true"},"invokedBy":"AWS Internal"},"eventTime":"2025-04-02T20:54:47Z","eventSource":"kms.amazonaws.com","eventName":"GenerateDataKey","awsRegion":"ap-south-1","sourceIPAddress":"AWS Internal","userAgent":"AWS Internal","requestParameters":{"keyId":"arn:aws:kms:ap-south-1:908027405956:key/d0a4851f-c4fc-4c82-a0e6-1681331a9a24","encryptionContext":{"aws:s3:arn":"arn:aws:s3:::bucket-lab9-2265"},"keySpec":"AES_256"},"responseElements":null,"requestID":"08bb12ed-c9c4-4d6f-b3e7-5d6c8ac36615","eventID":"67f2c8c8-3f49-4238-bb1b-827c9f8c88f1","readOnly":true,"resources":[{"accountId":"908027405956","type":"AWS::KMS::Key","ARN":"arn:aws:kms:ap-south-1:908027405956:key/d0a4851f-c4fc-4c82-a0e6-1681331a9a24"}],"eventCategory":"Management","eventVersion":"1.10","userIdentity":
```