

Cloud Security Implementation Report – Task 4

Organization: **CODTECH IT SOLUTIONS PVT. LTD.**

Intern Name: **Harshada D Jagtap**

Project Title: **IAM, Secure Storage, and Encryption on AWS**

Internship Duration: May 20, 2025 – July 20, 2025

1. Objective

This document outlines the implementation of AWS IAM (Identity and Access Management) policies, S3 secure storage, and encryption mechanisms as part of Task 4 during the Cloud Computing Internship at CODTECH IT SOLUTIONS PVT. LTD.

2. IAM Policy Implementation

- Created an IAM user `secure-user` with programmatic and console access.

The screenshot displays the AWS IAM console interface. The left-hand navigation pane shows the 'Identity and Access Management (IAM)' section, with 'Users' selected. The main content area shows the details for a user named 'cloud-intern'. The 'Summary' section includes the user's ARN, console access status (Enabled without MFA), and the creation date. The 'Permissions policies' section shows a list of policies attached to the user, including 'S3ReadOnlyPolicy'. The bottom of the console shows the 'CloudShell' button and the 'Feedback' link.

cloud-intern Info [Delete](#)

Summary

ARN: [arn:aws:iam::891612580419:user/cloud-intern](#)

Console access: [Enabled without MFA](#)

Access key 1: [Create access key](#)

Created: July 06, 2025, 18:50 (UTC+05:30)

Last console sign-in: [Never](#)

Permissions policies (3) [Remove](#) [Add permissions](#)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: [Customer inline](#) 1 match

Policy name	Type	Attached via
S3ReadOnlyPolicy	Customer inline	Inline

- Assigned a custom IAM policy with least privilege access to only one S3 bucket.

IAM Policy JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket", "s3:GetObject", "s3:PutObject"],
      "Resource": [
        "arn:aws:s3:::secure-storage-demo",
        "arn:aws:s3:::secure-storage-demo/*"
      ]
    }
  ]
}
```

The screenshot shows the AWS IAM console interface during the 'Review and create' step of creating a new policy. The breadcrumb navigation at the top indicates the path: IAM > Users > cloud-intern > Create policy. On the left, a progress bar shows 'Step 1: Specify permissions' and 'Step 2: Review and create' (the current step). The main content area is titled 'Review and create' with an 'Info' link. Below the title, it says 'Review the permissions, specify details, and tags.' The 'Policy details' section contains a 'Policy name' field with the value 'S3ReadOnlyPolicy' and a note: 'Enter a meaningful name to identify this policy. Maximum 128 characters. Use alphanumeric and '+=, @-_' characters.' The 'Permissions defined in this policy' section includes an 'Edit' button and a search bar. Below the search bar, it says 'Allow (1 of 444 services)' and a toggle for 'Show remaining 443 services'. A table lists the permissions:

Service	Access level	Resource	Request condition
S3	Limited: List, Read	Multiple	None

At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Create policy' (highlighted in orange). The footer contains 'CloudShell', 'Feedback', '© 2025, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

3. Secure S3 Bucket Configuration

- Created S3 bucket named `secure-storage-demo`.
- Chose AWS-Managed Keys (SSE-S3) or Customer-Managed Keys (SSE-KMS).

The screenshot shows the 'Create bucket' page in the AWS S3 console. The breadcrumb navigation is 'Amazon S3 > Buckets > Create bucket'. A message states 'You can add up to 50 tags.' The 'Default encryption' section indicates that server-side encryption is automatically applied. Under 'Encryption type', 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' is selected. Other options include 'Server-side encryption with AWS Key Management Service keys (SSE-KMS)' and 'Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)'. The 'Bucket Key' section has 'Enable' selected. An 'Advanced settings' section is collapsed. A light blue box at the bottom states: 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.'

The screenshot shows the 'secure-storage-demo-codtech' bucket page in the AWS S3 console. The breadcrumb navigation is 'Amazon S3 > Buckets > secure-storage-demo-codtech'. The 'Objects' tab is active, showing a table with one object: 'CLOUD COMPUTING.pdf'. The table columns are Name, Type, Last modified, Size, and Storage class. The object was last modified on July 6, 2025, at 19:01:09 (UTC+05:30) and has a size of 807.9 KB, stored in the Standard storage class. Above the table, there are buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload'.

Name	Type	Last modified	Size	Storage class
CLOUD COMPUTING.pdf	pdf	July 6, 2025, 19:01:09 (UTC+05:30)	807.9 KB	Standard

5. Testing & Validation

- Open a private/incognito browser.
- Use the IAM login URL.
- Log in as **cloud-intern-user**.

Amazon S3

Account snapshot - updated every 24 hours All AWS Regions View Storage Lens dashboard

Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. [Learn more](#)

General purpose buckets Directory buckets

General purpose buckets (1/2) Info All AWS Regions

Copy ARN Empty Delete Create bucket

Buckets are containers for data stored in S3.

secure-storage-demo-codtech 1 match

Name	AWS Region	IAM Access Analyzer	Creation date
secure-storage-demo-codtech	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	July 6, 2025, 19:00:22 (UTC+05:30)

Block Public Access settings for this account

Storage Lens

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

- Try to list objects from the bucket.

aws IAM Dashboard

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings
- Root access management New

Access reports

- Access Analyzer
- Resource analysis New

IAM Dashboard Info

Security recommendations 0

Access denied

You don't have permission to `iam:GetAccountSummary`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: `arn:aws:iam::891612580419:user/cloud-intern`

Action: `iam:GetAccountSummary`

Context: no identity-based policy allows the action

Diagnose with Amazon Q

Access denied

You don't have permission to `iam:ListMFADevices`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

Access denied

You don't have permission to `iam:ListAccountAliases`. To request access, copy the following text and send it to your AWS administrator. [Learn more about troubleshooting access denied errors.](#)

User: `arn:aws:iam::891612580419:user/cloud-intern`

Action: `iam:ListAccountAliases`

Context: no identity-based policy allows the action

Diagnose with Amazon Q

CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

7. Conclusion

The implementation ensured secure cloud storage using AWS best practices. IAM policies enforced access control, S3 configuration enabled encrypted storage. This setup demonstrates a practical understanding of cloud security principles.