

Aim -

To study and Implement Storage as a Service using Own Cloud/ AWS, Glaciers.

Theory -

What is Storage as a Service(STaaS)?

Storage as a Service (STaaS) is a cloud computing model that provides users with on-demand access to storage resources over the internet. In STaaS, users can store, access, and manage data in a remote storage infrastructure maintained by a third-party service provider, eliminating the need for users to invest in and maintain their own storage hardware and infrastructure.

Advantages:

- Cost Efficiency: STaaS follows a pay-as-you-go pricing model, where users only pay for the storage resources they consume. This eliminates the need for upfront investment in hardware and infrastructure, reducing capital expenditure and enabling cost-effective scaling based on demand.
- Scalability: STaaS platforms offer scalability features that allow users to easily scale their storage resources up or down based on changing requirements. This elasticity enables organizations to accommodate growing data volumes and fluctuating storage needs without the need for manual intervention.
- Reduced Management Overhead: STaaS abstracts the complexity of managing storage infrastructure, including hardware provisioning, software installation, data replication, backup, and maintenance. This reduces administrative overhead and allows organizations to focus on their core business activities rather than storage management tasks.
- High Availability and Data Durability: Many STaaS providers offer built-in redundancy, data replication, and backup capabilities to ensure high availability and data durability. This helps protect against data loss and ensures continuous access to data even in the event of hardware failures or disasters.
- Accessibility and Anywhere Access: STaaS enables users to access and manage their data from anywhere with an internet connection, providing flexibility and convenience for remote work, collaboration, and data sharing across distributed teams and locations.

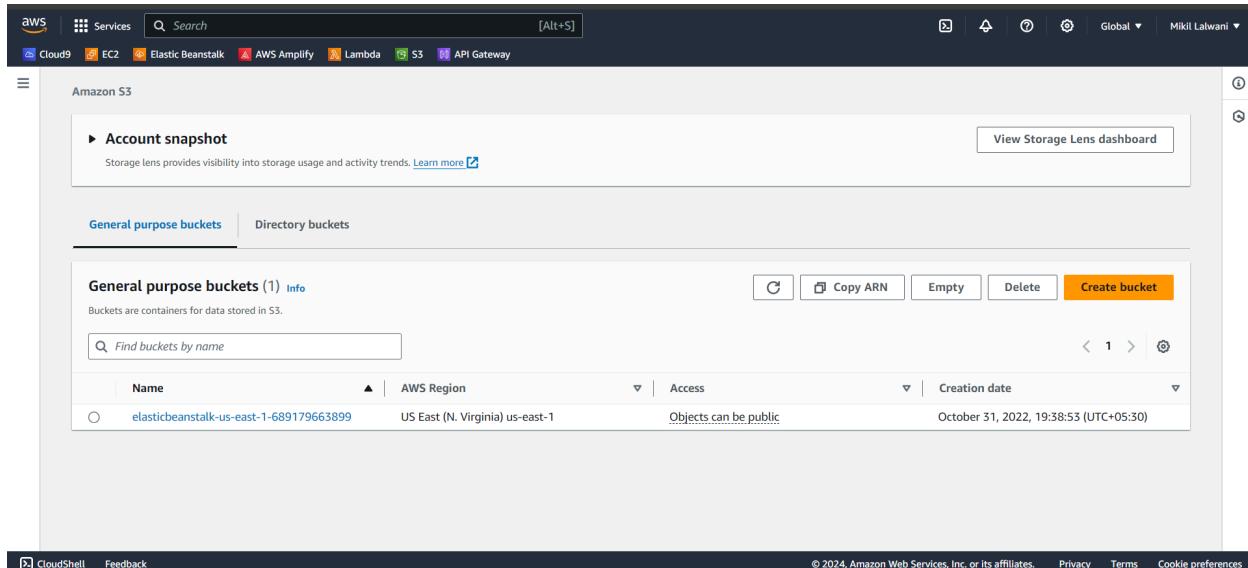
Disadvantages:

- Security and Privacy Concerns: Storing sensitive data in a third-party cloud environment raises concerns about data security and privacy. Organizations must carefully evaluate the security measures implemented by STaaS providers to ensure compliance with regulatory requirements and protect their data from unauthorized access and breaches.

- Dependency on Internet Connectivity: STaaS relies on internet connectivity for accessing and managing storage resources, which may pose challenges in environments with limited or unreliable internet connectivity. Organizations should consider the potential impact of internet outages or disruptions on their data access and storage operations.
- Data Transfer Costs: Transferring large volumes of data to and from STaaS platforms may incur additional data transfer costs, particularly for organizations with high data volumes or frequent data migrations. Organizations should carefully consider data transfer costs when evaluating the total cost of ownership of STaaS solutions.
- Vendor Lock-In: Migrating data between different STaaS providers or transitioning from STaaS to an on-premises storage deployment may be challenging and costly, leading to vendor lock-in. Organizations should consider the long-term implications of vendor lock-in and evaluate strategies to mitigate this risk.
- Performance and Latency: Performance and latency issues may arise in STaaS environments, particularly in multi-tenant deployments where resources are shared among multiple users. Organizations should assess the performance characteristics of STaaS offerings and ensure they meet their performance requirements before migration.

Procedure -

Step-1: click on create bucket



The screenshot shows the AWS S3 console. At the top, there's a navigation bar with links for Cloud9, EC2, Elastic Beanstalk, AWS Amplify, Lambda, S3, and API Gateway. Below the navigation bar, the title 'Amazon S3' is displayed. On the left, there's a sidebar with a 'General purpose buckets' section containing a table with one row. The table has columns for 'Name', 'AWS Region', 'Access', and 'Creation date'. The single row shows 'elasticbeanstalk-us-east-1-689179663899' under 'Name', 'US East (N. Virginia) us-east-1' under 'AWS Region', 'Objects can be public' under 'Access', and 'October 31, 2022, 19:38:53 (UTC+05:30)' under 'Creation date'. To the right of the table, there are buttons for 'Create bucket' (highlighted with a yellow box), 'Copy ARN', 'Empty', and 'Delete'. At the bottom of the page, there are links for 'CloudShell', 'Feedback', '© 2024, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

Step-2: Give Bucket name & select region for storage

The screenshot shows the 'General configuration' step of the 'Create Bucket' wizard. It includes fields for 'Bucket name' (mikil_ccl), 'AWS Region' (US East (N. Virginia) us-east-1), and 'Bucket type' (set to 'General purpose'). A note explains that general purpose buckets are the original S3 bucket type and provide redundancy across multiple Availability Zones. There is also a section for 'Copy settings from existing bucket - optional'.

Step-3: Keep object ownership setting as ACLs Disabled as by-default

The screenshot shows the 'Object Ownership' configuration page. The 'ACLs disabled (recommended)' option is selected, indicating that all objects in the bucket are owned by the account owner and access is controlled by policies. Below this, under 'Block Public Access settings for this bucket', the 'Block all public access' checkbox is checked. A note states that turning this setting on is equivalent to enabling four other settings: blocking public access to the bucket, objects, and grants, and disabling cross-account public access.

Step-4: Disable block all public access checkbox

The screenshot shows the AWS S3 console with the 'Block Public Access' tab selected. At the top, it says 'Object Ownership' and 'Bucket owner enforced'. Below that, a section titled 'Block Public Access settings for this bucket' contains a note about public access being granted through various controls like ACLs and policies. It includes a checkbox for 'Block all public access' and four detailed sub-options under it. At the bottom, there's a note about turning off block all public access potentially making the bucket public, followed by an acknowledgement checkbox.

Block all public access

- Block public access to buckets and objects granted through new access control lists (ACLs)
- Block public access to buckets and objects granted through any access control lists (ACLs)
- Block public access to buckets and objects granted through new public bucket or access point policies
- Block public and cross-account access to buckets and objects through any public bucket or access point policies

Turning off block all public access might result in this bucket and the objects within becoming public

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Step-5: Select the checkbox for Turning off block all public access might result in this bucket and the objects within becoming public

The screenshot shows the AWS S3 console with the 'Bucket Versioning' tab selected. It displays a note about versioning and its purpose. Below the note is a checkbox for acknowledging potential public access if versioning is disabled.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore

I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Step-6: Keep bucket versioning as disabled and add tags if required.

Bucket Versioning
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
 Disable
 Enable

Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.
[Add tag](#)

Default encryption [Info](#)
Server-side encryption is automatically applied to new objects stored in this bucket.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step-7: Keep default encryption and click on create bucket button

NO tags associated with this bucket.
[Add tag](#)

Default encryption [Info](#)
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](#).

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

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

You can now see the successful creation of your bucket

The screenshot shows the AWS S3 buckets page. At the top, there's a green success message: "Successfully created bucket 'mikil-ccl'. To upload files and folders, or to configure additional bucket settings, choose View details." Below this, the "Account snapshot" section is visible, followed by the "General purpose buckets" section. There are two buckets listed:

Name	AWS Region	Access	Creation date
elasticbeanstalk-us-east-1-689179663899	US East (N. Virginia) us-east-1	Objects can be public	October 31, 2022, 19:38:53 (UTC+05:30)
mikil-ccl	US East (N. Virginia) us-east-1	Objects can be public	March 16, 2024, 09:15:30 (UTC+05:30)

Step-8: Now click on the bucket that you have created.

This screenshot is identical to the one above, showing the AWS S3 buckets page with the same two buckets listed: "elasticbeanstalk-us-east-1-689179663899" and "mikil-ccl". The "mikil-ccl" bucket was created in Step 8.

Step-9: You can either create a folder here or upload an existing file in the bucket

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and various service links like Cloud9, EC2, Elastic Beanstalk, AWS Amplify, Lambda, S3, and API Gateway. Below the navigation bar, the path 'Amazon S3 > Buckets > mikil-ccl' is displayed. The main content area is titled 'mikil-ccl info'. There are tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points', with 'Objects' being the active tab. Under the 'Objects' tab, there's a heading 'Objects (0) Info'. A toolbar below this includes buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and a large orange 'Upload' button. A search bar labeled 'Find objects by prefix' is present. A table header row shows columns for 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. The main body of the table is empty and displays the message 'No objects. You don't have any objects in this bucket.' At the bottom right of the table is another orange 'Upload' button. The footer of the page includes links for CloudShell, Feedback, and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

Step-10: now click on upload button and click on add files button browse your local machine and select which file you need to upload on S3 next click on upload button at bottom right end

The screenshot shows the 'Upload' screen for the 'mikil-ccl' bucket. The path 'Amazon S3 > Buckets > mikil-ccl > Upload' is visible at the top. The main title is 'Upload info'. A sub-instruction says 'Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more' with a link. Below this is a large dashed blue rectangular area with the placeholder text 'Drag and drop files and folders you want to upload here, or choose Add files or Add folder.' A 'Files and folders (0)' section follows, containing a 'Remove' button and 'Add files' and 'Add folder' buttons. A search bar 'Find by name' is present. A table with columns 'Name', 'Folder', and 'Type' shows 'No files or folders' and the message 'You have not chosen any files or folders to upload.' The footer includes links for CloudShell, Feedback, and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences'.

Now you can check the upload status screen

The screenshot shows the AWS S3 console with a green success message at the top: "Upload succeeded" and "View details below." Below this, there's a summary table with one row: Destination s3://mikil-ccl, Status Succeeded (1 file, 0 B (0%)), and Failed (0 files, 0 B (0%)). Under the "Files and folders" tab, a table lists one item: mikil_test_file.docx, which is an application file of size 0 B and status Succeeded. The bottom navigation bar includes CloudShell, Feedback, and links to Privacy, Terms, and Cookie preferences.

Now click on close button
The screen will appear as below

The screenshot shows the AWS S3 console with the path Amazon S3 > Buckets > mikil-ccl. The "Objects" tab is selected, showing a single object: mikil_test_file.docx, which is a docx file last modified on March 16, 2024, at 09:17:58 (UTC+05:30), with a size of 0 B and a storage class of Standard. The top navigation bar includes CloudShell, Feedback, and links to Privacy, Terms, and Cookie preferences.

Step-11: Select properties and scroll down to Static website hosting option which is disabled now click on Edit option on right side

The screenshot shows the AWS S3 bucket properties page for a bucket named 'aws-tutorial'. The 'Static website hosting' section is expanded, showing the following configuration:

- Index document:**
- Error document - optional:**
- Redirection rules - optional:** A JSON editor interface is shown, currently empty.

At the bottom of the page, there are links for CloudShell, Feedback, and a footer with copyright information and links to Privacy, Terms, and Cookie preferences.

Step-12: Enable the radio button and specify the file name in Index document which you have added in S3

The screenshot shows the AWS S3 bucket properties page for a bucket named 'aws-tutorial'. The 'Static website hosting' section is expanded, showing the following configuration:

- Index document:**
- Error document - optional:**
- Redirection rules - optional:** A JSON editor interface is shown, currently empty.

At the bottom of the page, there are links for CloudShell, Feedback, and a footer with copyright information and links to Privacy, Terms, and Cookie preferences.

The screenshot shows the AWS Management Console with the AWS logo and a search bar at the top. Below the search bar, there are links for Cloud9, EC2, Elastic Beanstalk, AWS Amplify, Lambda, S3, and API Gateway. On the far right, it shows 'Global' and 'Mikil Lalwani'. The main navigation bar has 'Amazon S3' selected, followed by 'Buckets' and 'mikil-ccl'. The current page is 'Edit static website hosting'.

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

Disable
 Enable

Hosting type

Host a static website
Use the bucket endpoint as the web address. [Learn more](#)
 Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

Index document

Specify the home or default page of the website.

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Scroll down and save the changes at bottom right
Following screen will appear

The screenshot shows the AWS Management Console with the AWS logo and a search bar at the top. Below the search bar, there are links for Cloud9, EC2, Elastic Beanstalk, AWS Amplify, Lambda, S3, and API Gateway. On the far right, it shows 'Global' and 'Mikil Lalwani'. The main navigation bar has 'Amazon S3' selected, followed by 'Buckets' and 'mikil-ccl'. The current page is 'Properties'.

Successfully edited static website hosting.

mikil-ccl [Info](#)

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

Bucket overview

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN) arn:aws:s3:::mikil-ccl	Creation date March 16, 2024, 09:15:30 (UTC+05:30)
---	--	---

Bucket Versioning

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
Disabled
Multi-factor authentication (MFA) delete

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Step-13: Click on Permissions Tab

mikil-ccl [info](#)

Objects Properties **Permissions** Metrics Management Access Points

Permissions overview

Access
Objects can be public

Block public access (bucket settings)

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 all your S3 buckets and 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 your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

⚠ Off

▶ Individual Block Public Access settings for this bucket

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step-14: In bucket policy click on Edit option

Cloud9 EC2 Elastic Beanstalk AWS Amplify Lambda S3 API Gateway

⚠ Off

▶ Individual Block Public Access settings for this bucket

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

No policy to display.

Edit Delete Copy

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 15- after clicking on edit button paste the following code in bucket policy

{

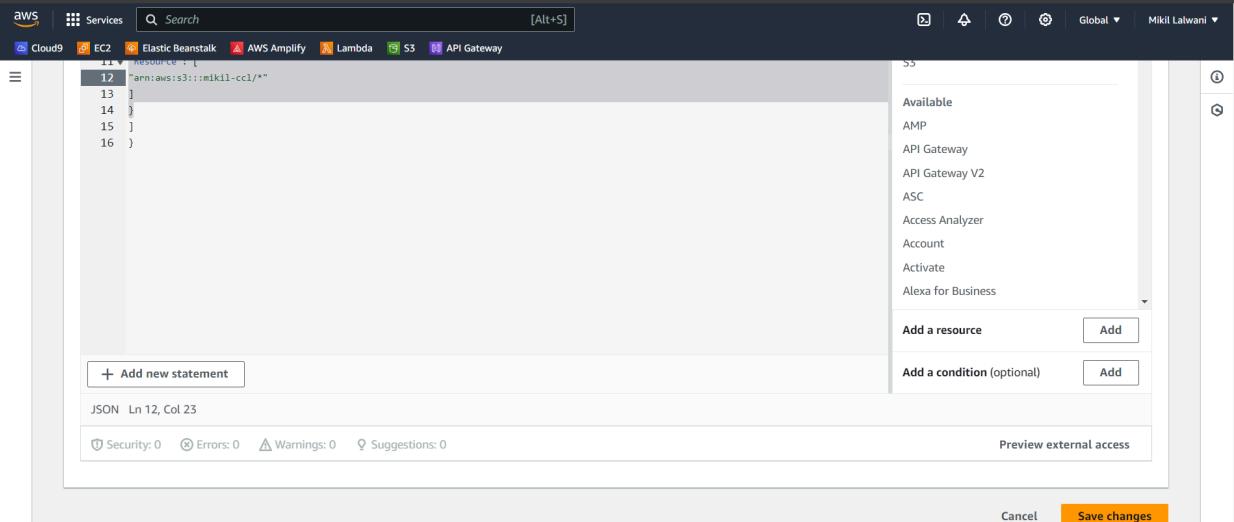
```
"Version": "2012-10-17",
"Statement": [
{
    "Sid": "PublicReadGetObject",
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
        "s3:GetObject"
```

```

        ],
      "Resource": [
        "arn:aws:s3:::Bucket-Name/*"
      ]
    }
  ]
}

```

Note-Make sure that you add your bucket name in the code above
 Scroll down and click on Save Changes button



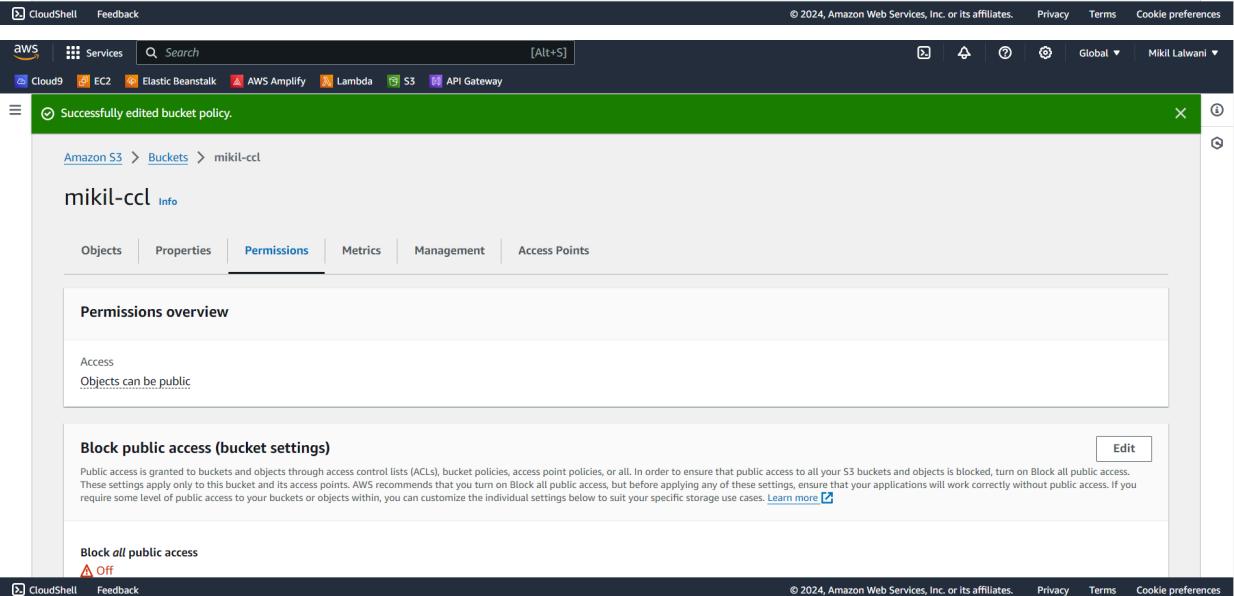
The screenshot shows the AWS IAM Policy Editor interface. The main area displays a JSON policy document:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::mikil-ccl/*"
    }
  ]
}

```

Below the policy editor, there are status indicators: Security: 0, Errors: 0, Warnings: 0, Suggestions: 0, and a 'Preview external access' link. At the bottom right, there are 'Cancel' and 'Save changes' buttons, with 'Save changes' being highlighted.



The screenshot shows the 'Permissions' tab selected in the Amazon S3 Bucket settings. The 'Block public access (bucket settings)' section is visible, containing a note about public access settings and a 'Edit' button. Below it, the 'Block all public access' setting is shown as 'Off'. The status bar at the bottom indicates the URL: [Amazon S3 > Buckets > mikil-ccl](#).

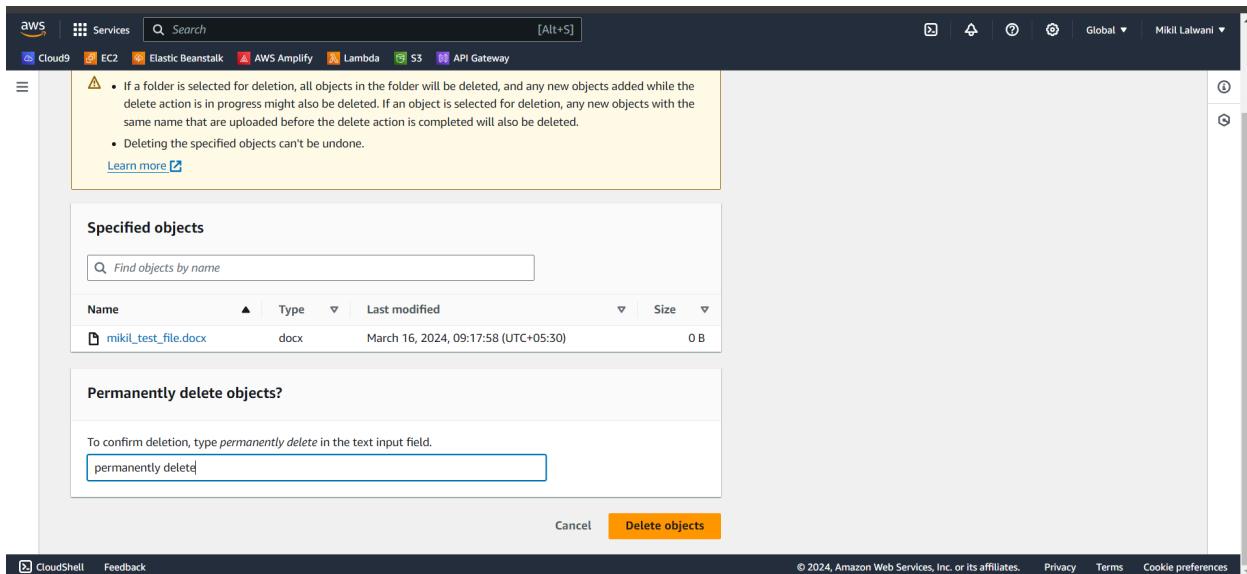
Step-16: open your html file and click on Object URL

The screenshot shows the AWS S3 Object Properties page for a file named 'mikil_test_file.docx'. The file was uploaded by 'mikil.lalwani03' from the 'US East (N. Virginia) us-east-1' region on March 16, 2024, at 09:17:58 (UTC+05:30). The file is a Microsoft Word document ('docx') type. The object key is 'mikil_test_file.docx'. The S3 URI is 's3://mikil-ccl/mikil_test_file.docx', and the ARN is 'arn:aws:s3:::mikil-ccl/mikil_test_file.docx'. The entity tag (Etag) is 'd41d8cd98f00b204e9800998ecf8427e', and the object URL is 'https://mikil-ccl.s3.amazonaws.com/mikil_test_file.docx'.

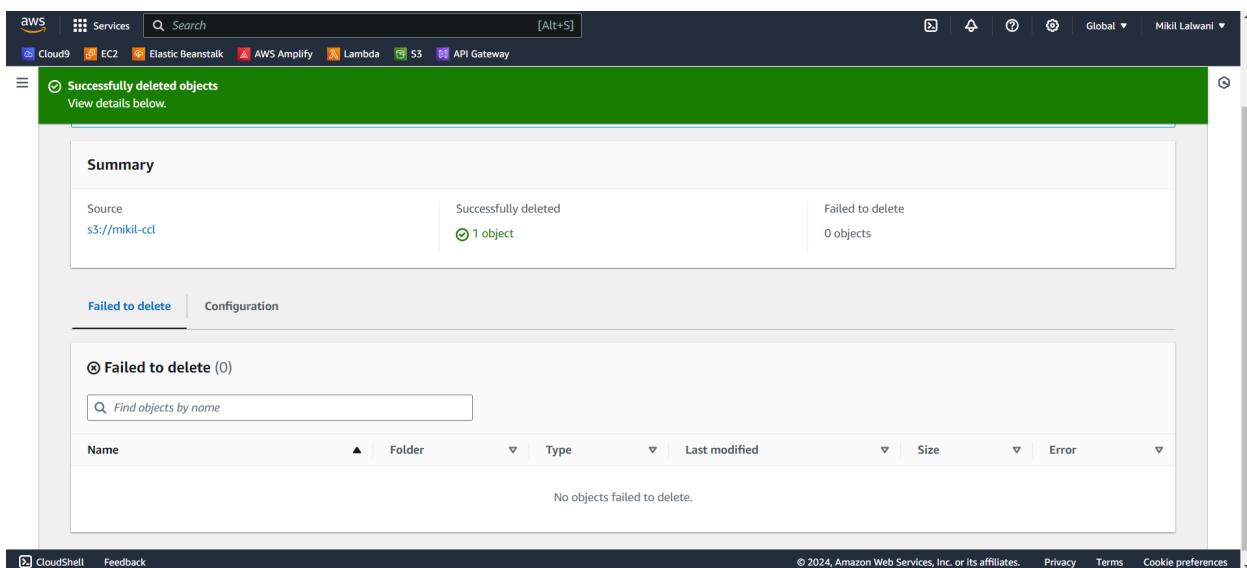
Step-17: Now for delete files click on checkbox of your file and then click on Delete Button

The screenshot shows the AWS S3 Bucket Objects page for the 'mikil-ccl' bucket. There is one object listed: 'mikil_test_file.docx', which is a Microsoft Word document ('docx') uploaded on March 16, 2024, at 09:17:58 (UTC+05:30). The file size is 0 B and it is stored in the Standard storage class. The 'Delete' button is highlighted in orange, indicating it is selected for deletion.

Write permanently delete and click on delete object button



Now click on close button



Step-18: now come to Amazon S3 tab and select your bucket and then click on delete button

The screenshot shows the AWS S3 Buckets page. On the left, a sidebar lists options like Buckets, Access Grants, and Storage Lens. The main area displays an account snapshot and a table of general purpose buckets. The table has columns for Name, AWS Region, Access, and Creation date. It shows two entries:

Name	AWS Region	Access	Creation date
elasticbeanstalk-us-east-1-689179663899	US East (N. Virginia) us-east-1	Objects can be public	October 31, 2022, 19:38:53 (UTC+05:30)
mikil-ccl	US East (N. Virginia) us-east-1	Objects can be public	March 16, 2024, 09:15:30 (UTC+05:30)

At the bottom right of the table, there are buttons for Copy ARN, Empty, Delete, and Create bucket.

Write down your bucket name in delete bucket tab and click on delete button at bottom right

The screenshot shows a 'Delete bucket' confirmation dialog. It contains a warning message about the不可逆性 of deleting buckets and a text input field where the bucket name 'mikil-ccl' is typed. At the bottom are 'Cancel' and 'Delete bucket' buttons.

You can see that the bucket is deleted

The screenshot shows the AWS S3 console. At the top, there's a green notification bar stating "Successfully deleted bucket 'mikil-cc!'" with a close button. Below it, the title "Amazon S3" is followed by a "Account snapshot" section with a "View Storage Lens dashboard" button. Under "General purpose buckets", there's a table with one row:

Name	AWS Region	Access	Creation date
elasticbeanstalk-us-east-1-689179663899	US East (N. Virginia) us-east-1	Objects can be public	October 31, 2022, 19:38:53 (UTC+05:30)

At the bottom, there are links for CloudShell, Feedback, and various AWS terms like Privacy, Terms, and Cookie preferences.

Conclusion -

Thus we have successfully studied and implemented Storage as a Service using AWS.