

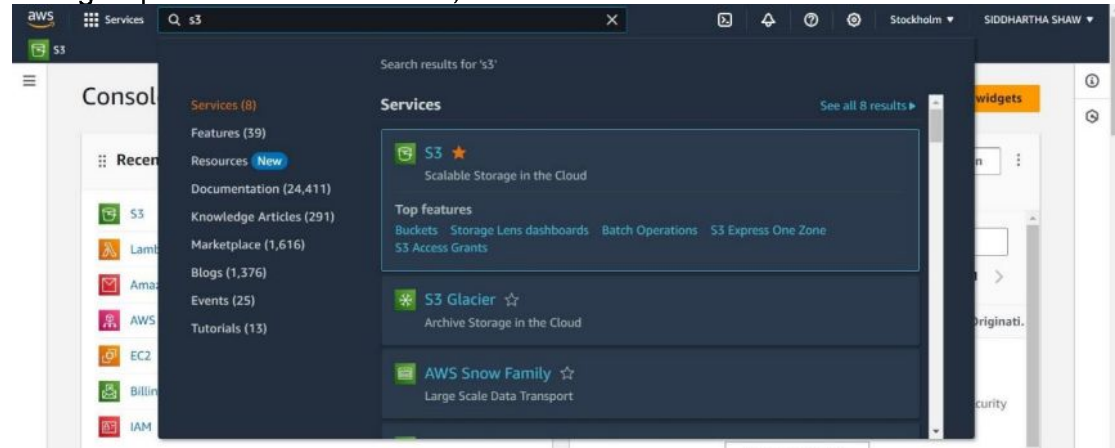
ASSIGNMENT- 5

PROBLEM STATEMENT :

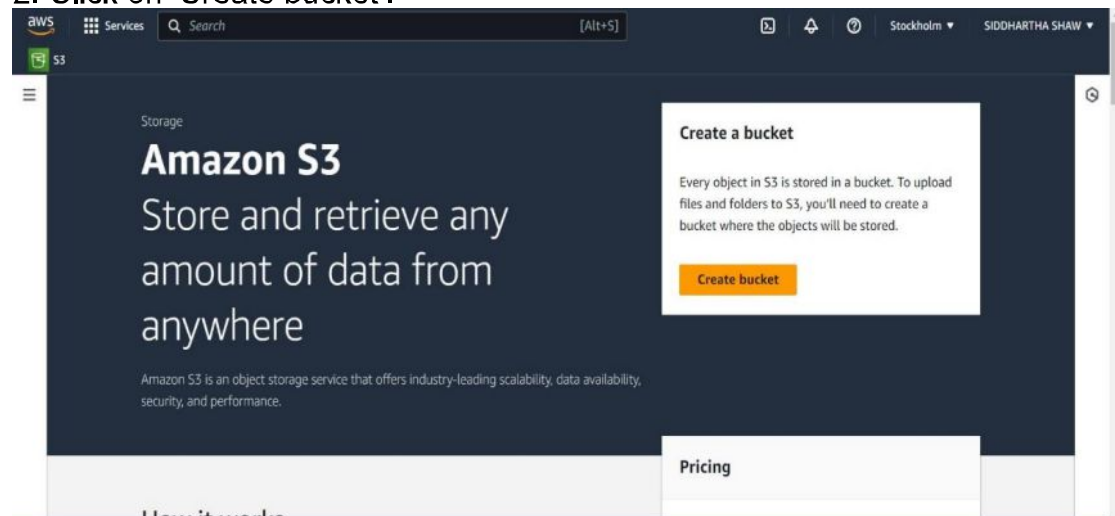
5) Create a public bucket in AWS. Upload a file and check by reassigned URL whether you can access the file or not.

Bucket creation and checking for access->

1. Sign up for an AWS account, search for 'S3' then click on it.



2. Click on 'Create bucket'.



3. Fill up the required details->'AWS region', 'Bucket name', click on 'ACLs enabled', uncheck 'Block all public access', tick off 'I acknowledge....' and click on 'Create bucket'.

AWS Region
Europe (Stockholm) eu-north-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.

☐ **Directory - New**
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name [Info](#)
siddKO467

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

☐ **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.

Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the

4. 'sidd2378' bucket is created successfully then click on the bucket name 'sidd2378'.

5. Under 'sidd2378', click on 'Upload' then choose a file of your choice and upload it.

Successfully created bucket "sidd2378"
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

[General purpose buckets](#) [Directory buckets](#)

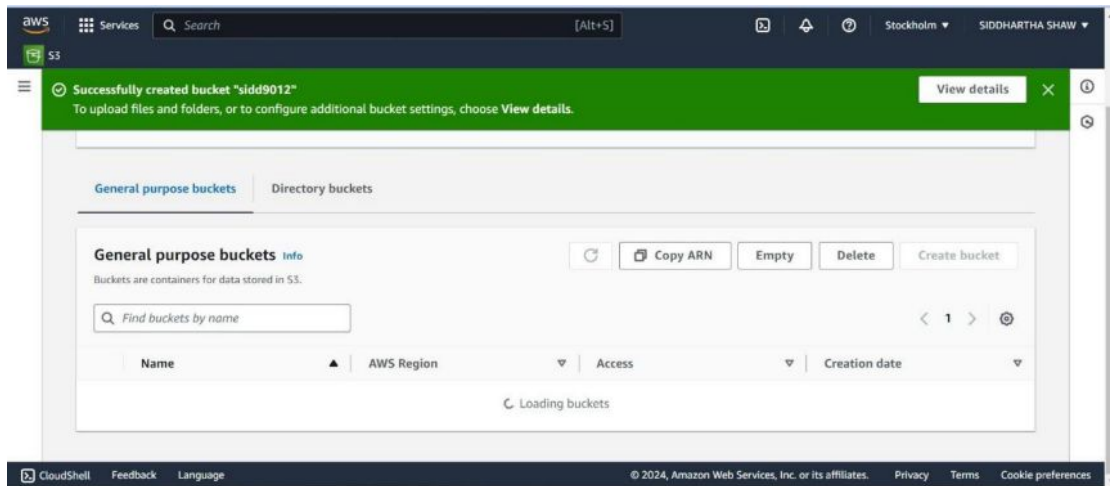
General purpose buckets (1) [Info](#)

Buckets are containers for data stored in S3.

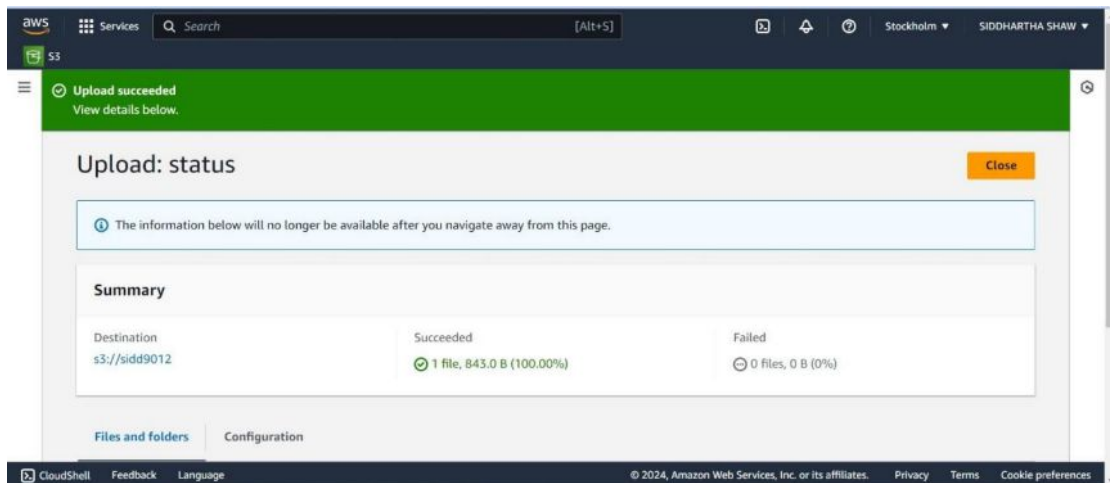
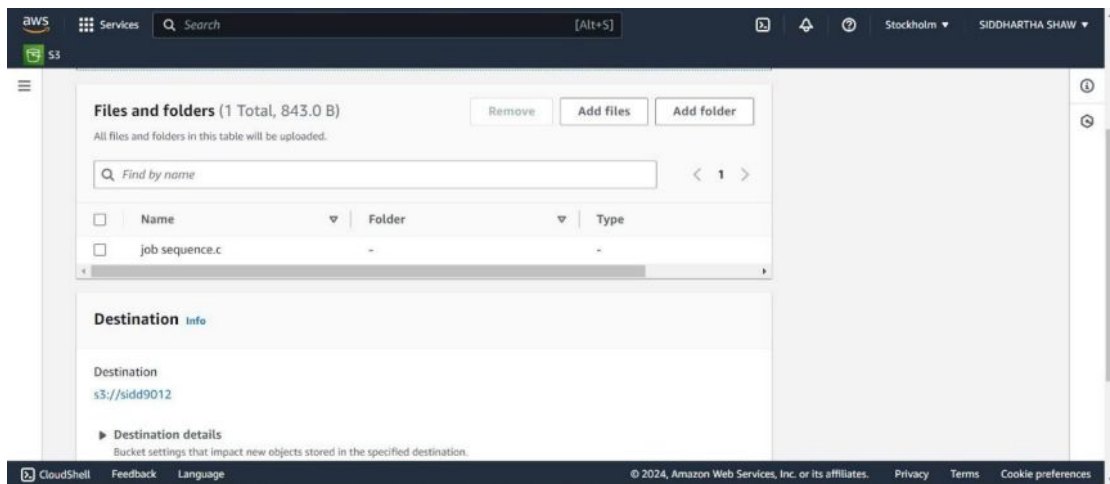
Name	AWS Region	Access	Creation date
<input type="radio"/> sidd2378	Europe (Stockholm) eu-north-1	Bucket and objects not public	April 4, 2024, 09:12:36 (UTC+05:30)

6. Click on 'Add files' then tick off the 'Name' of the file and click on 'Upload'.

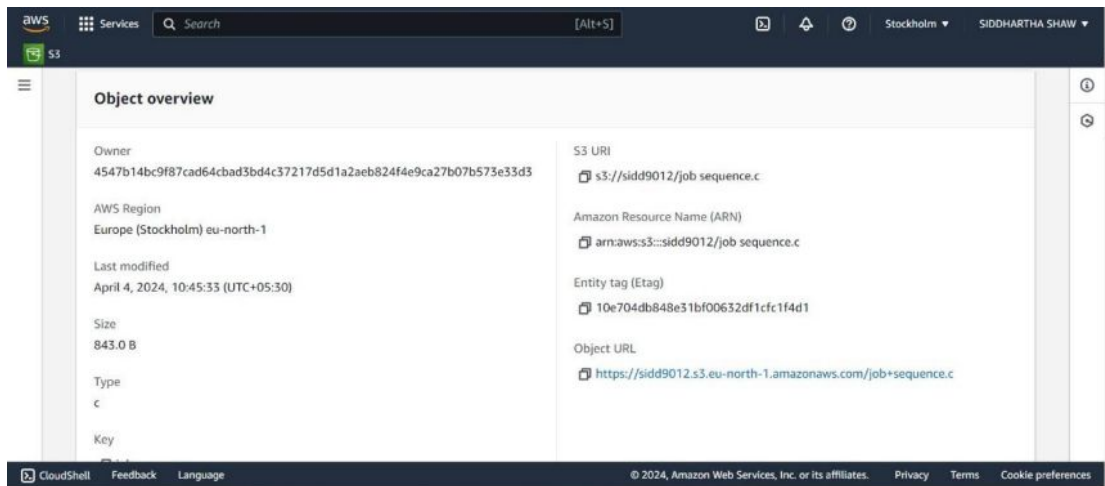
7. File is uploaded successfully, tap on 'Close' and click on 'Name'.



8. Under 'sidd2378', tick off any one of the file(checkbox) and click on the file.



9. Copy the 'Object URL'.



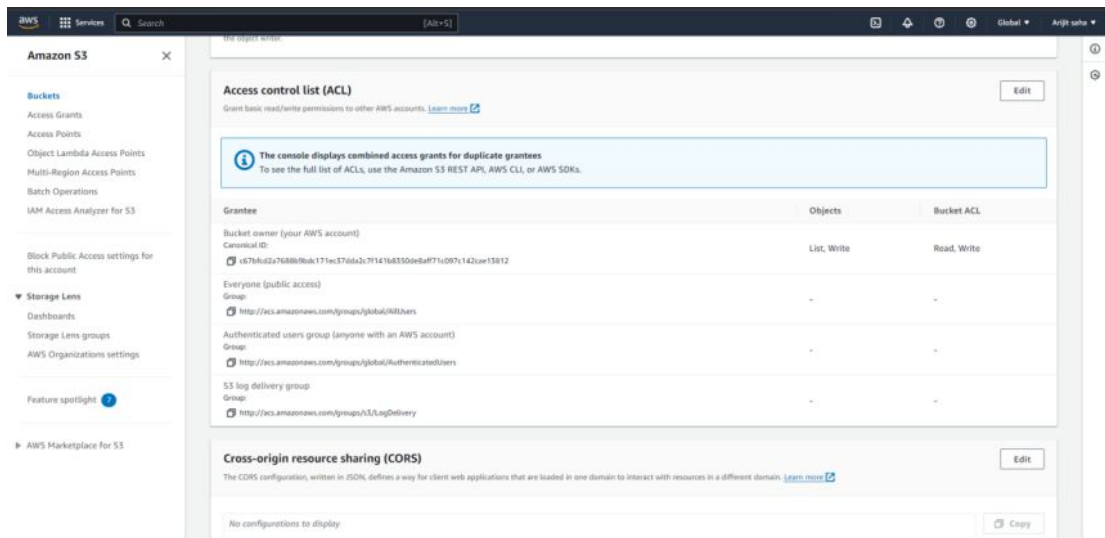
10. Now open the 'Incognito mode' and paste the 'Object URL'. You will see that the file cannot be accessed

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

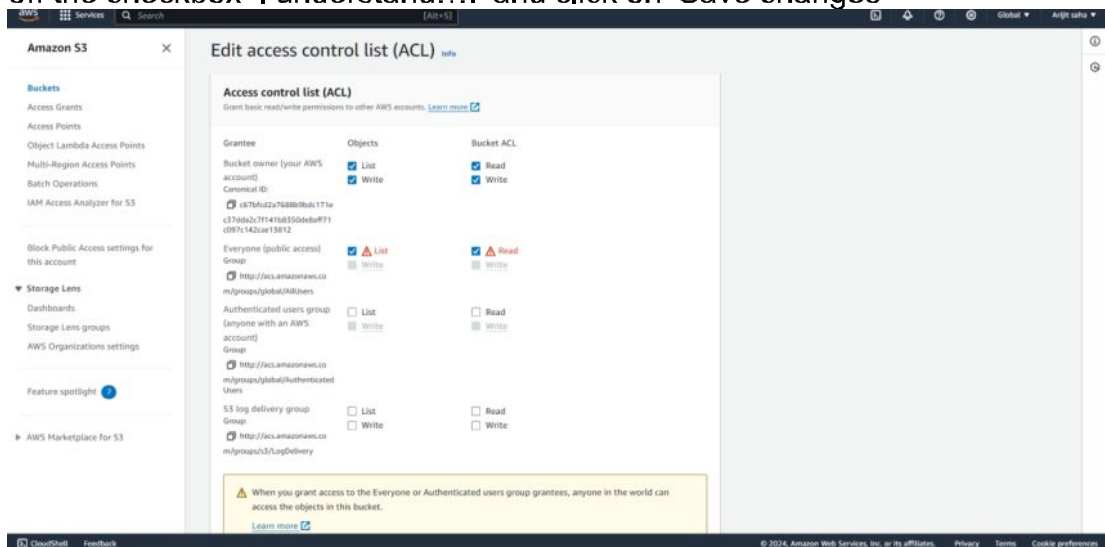
```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>QV5J11BVFN89AX</RequestId>
  <HostId>aV4k10RvuyTrvh2/VZqbekie8hL8Hpt/URfLSvzhdkbA0geR6e6Bjn9EPK+Qu1R1k+012/0Zf0=</HostId>
</Error>
```

To give access to the file , follow the steps given below.

11. In the file info. click on 'Permissions' and then click on 'Edit' beside 'Access control list(ACL)'.

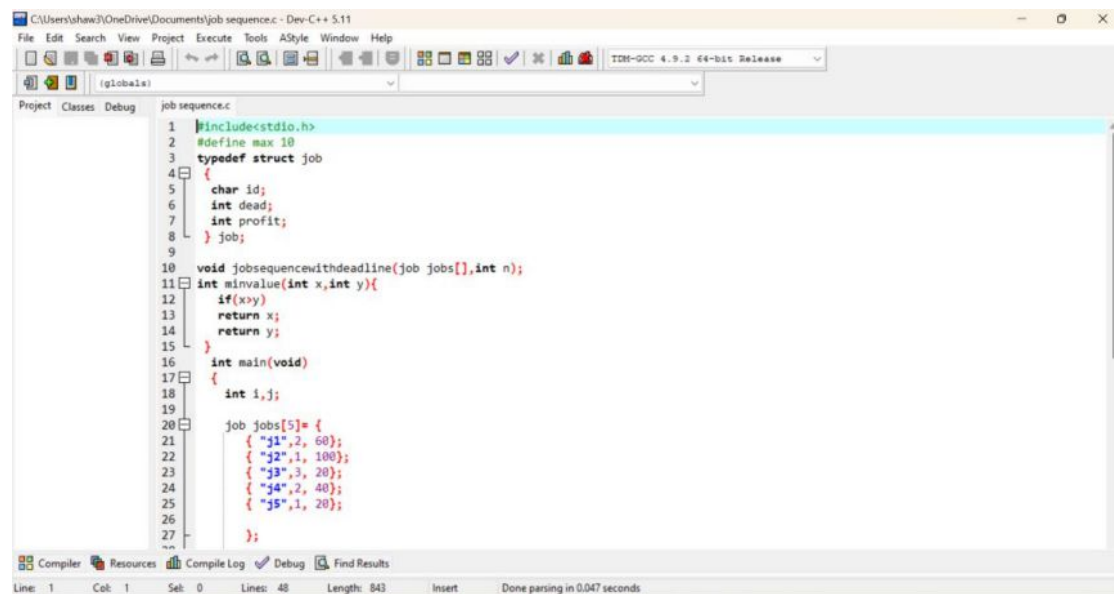


12. Now, tick off the Read checkboxes of 'Everyone(public access)', then tick off the checkbox 'I understand...' and click on 'Save changes'



13. Now, again copy the Object URL.

14. In the 'Incognito mode', paste the Object URL. We find that now the file can be accessed publicly.



```
1 |include<stdio.h>
2 |define max 10
3 |typedef struct job
4 |{
5 |    char id;
6 |    int dead;
7 |    int profit;
8 |} job;
9
10 |void jobsequencewithdeadline(job jobs[],int n);
11 |int minvalue(int x,int y){
12 |    if(x>y)
13 |        return x;
14 |    return y;
15 |}
16 |int main(void)
17 |{
18 |    int i,j;
19
20 |    job jobs[5]= {
21 |        {"j1",2, 60};
22 |        {"j2",1, 100};
23 |        {"j3",3, 20};
24 |        {"j4",2, 40};
25 |        {"j5",1, 20};
26 |    };
27 |}
```

Line: 1 Col: 1 Sel: 0 Lines: 48 Length: 843 Insert Done parsing in 0.047 seconds

15. delete the bucket from aws and return back to aws console.