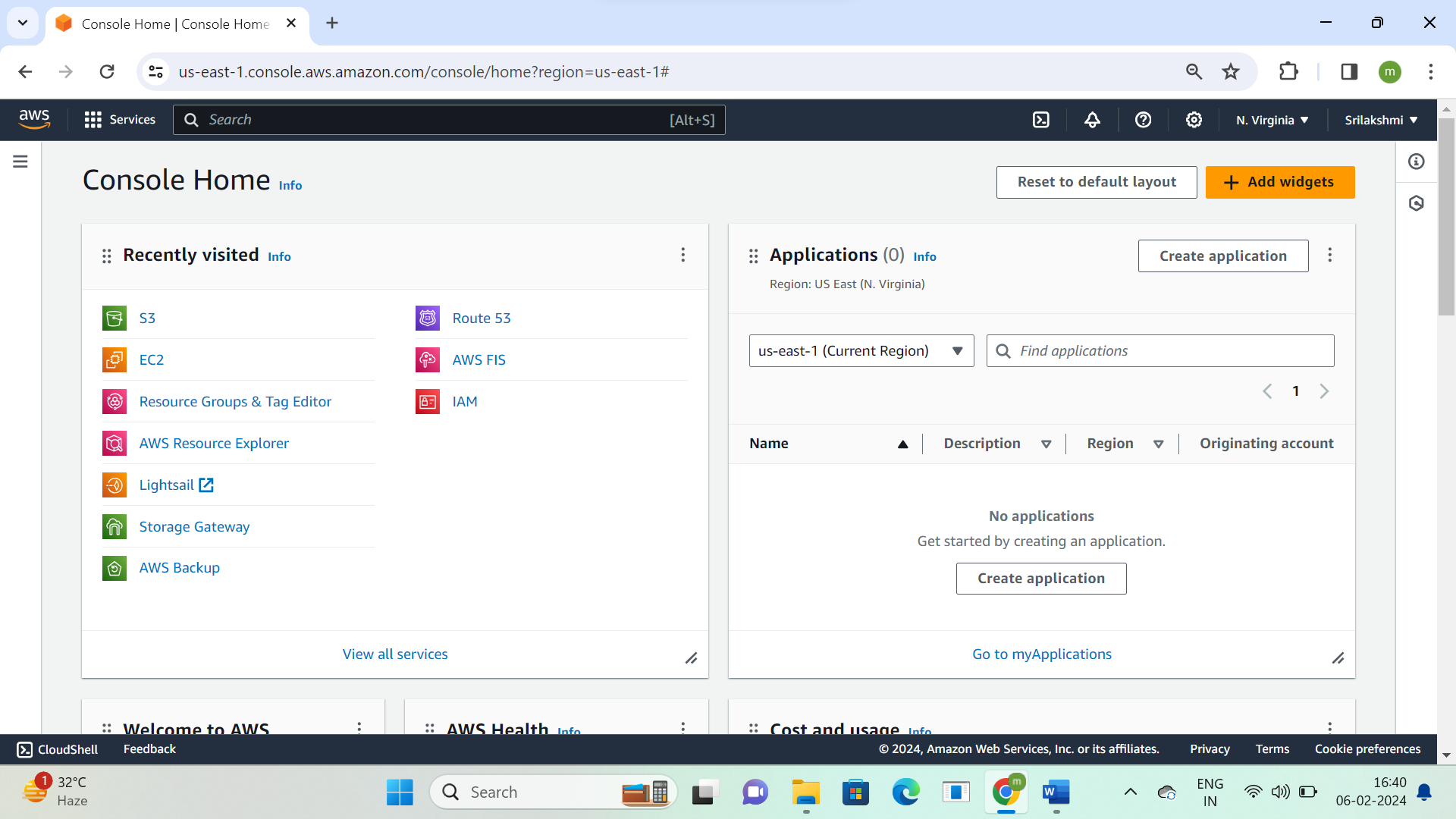
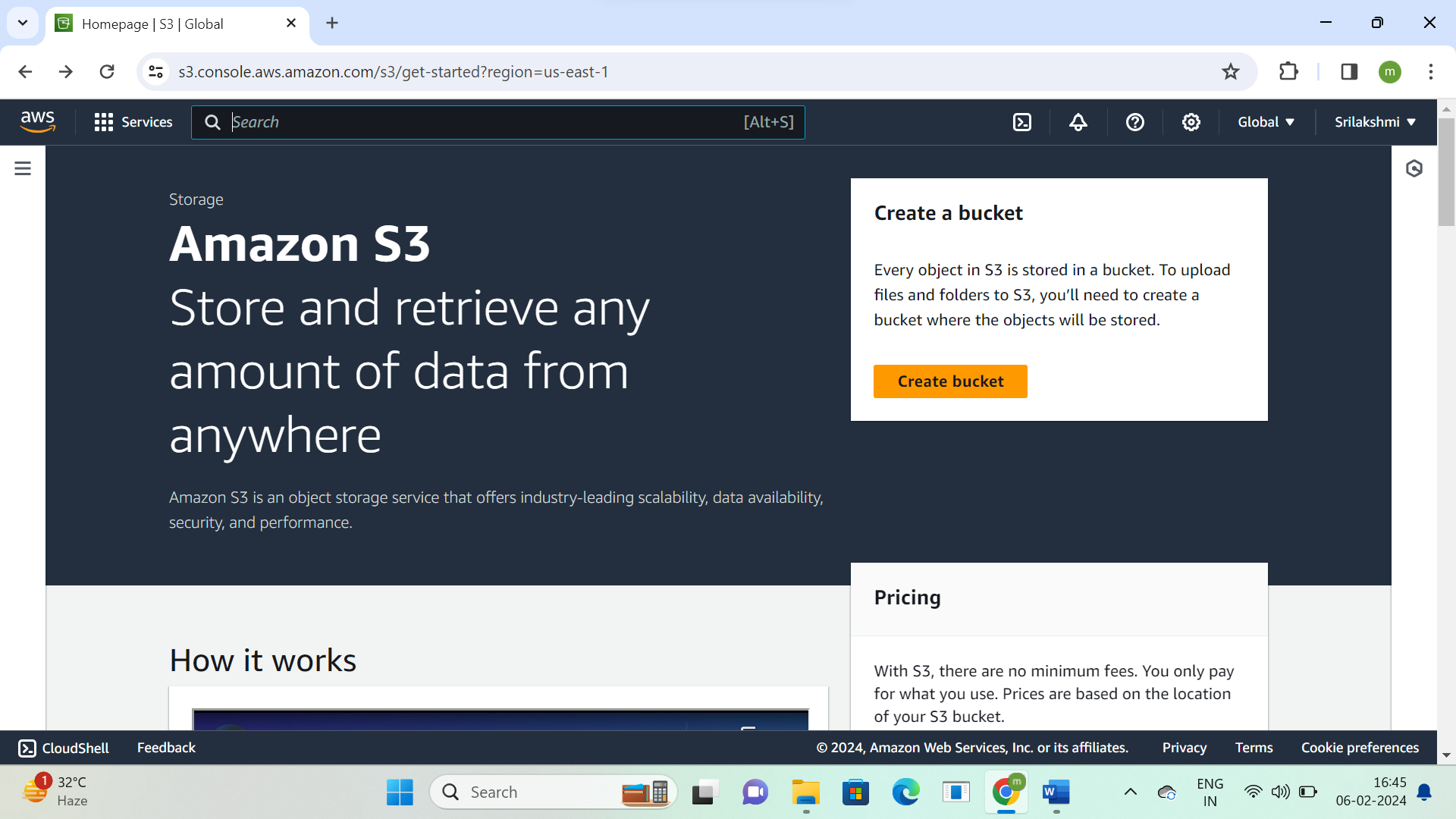
**Create a Storage account in any cloud AWS/Azure and try securing it to protect your data.**

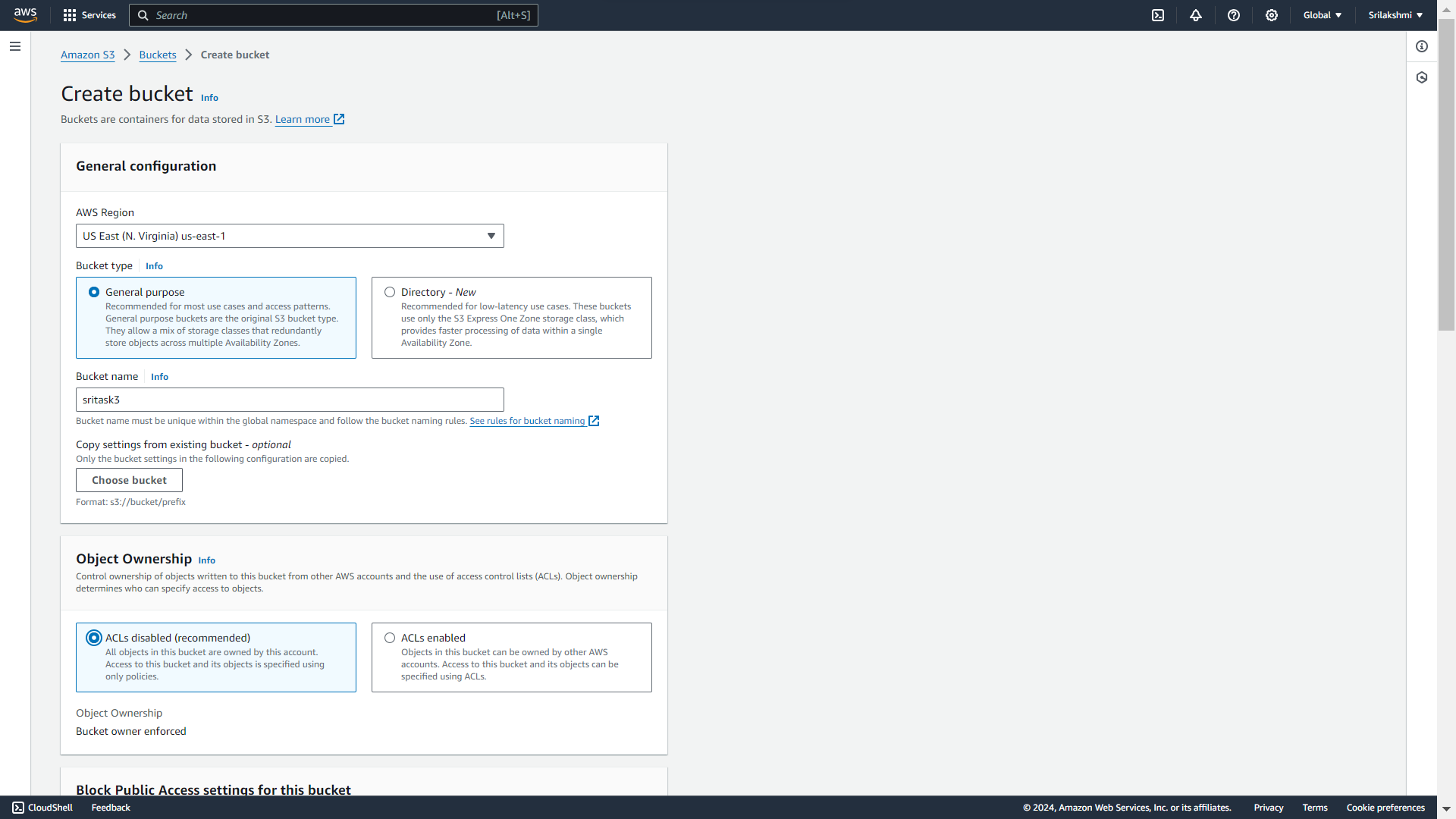
**Login to AWS console and select S3 bucket**



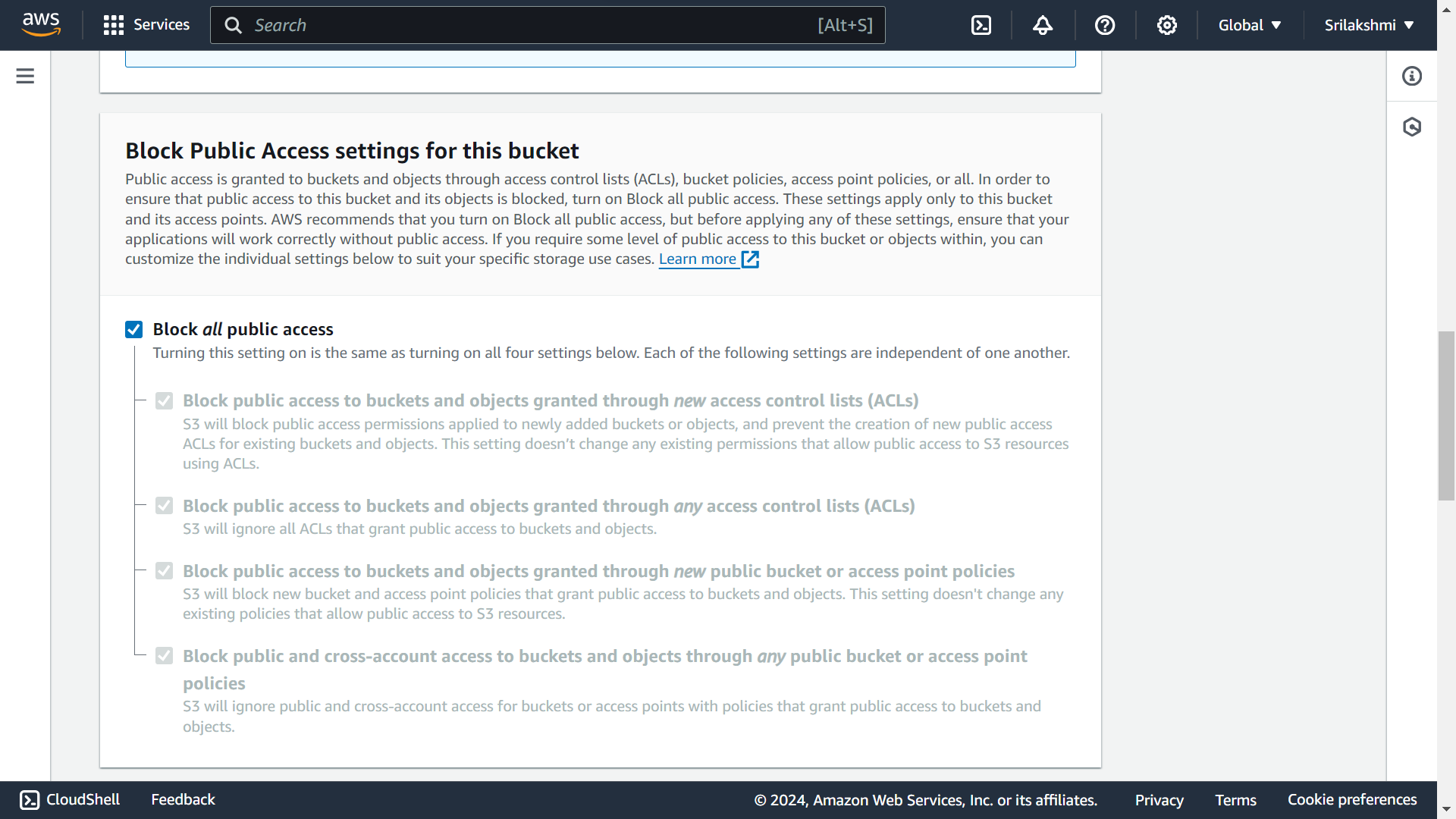
**Click on create bucket**



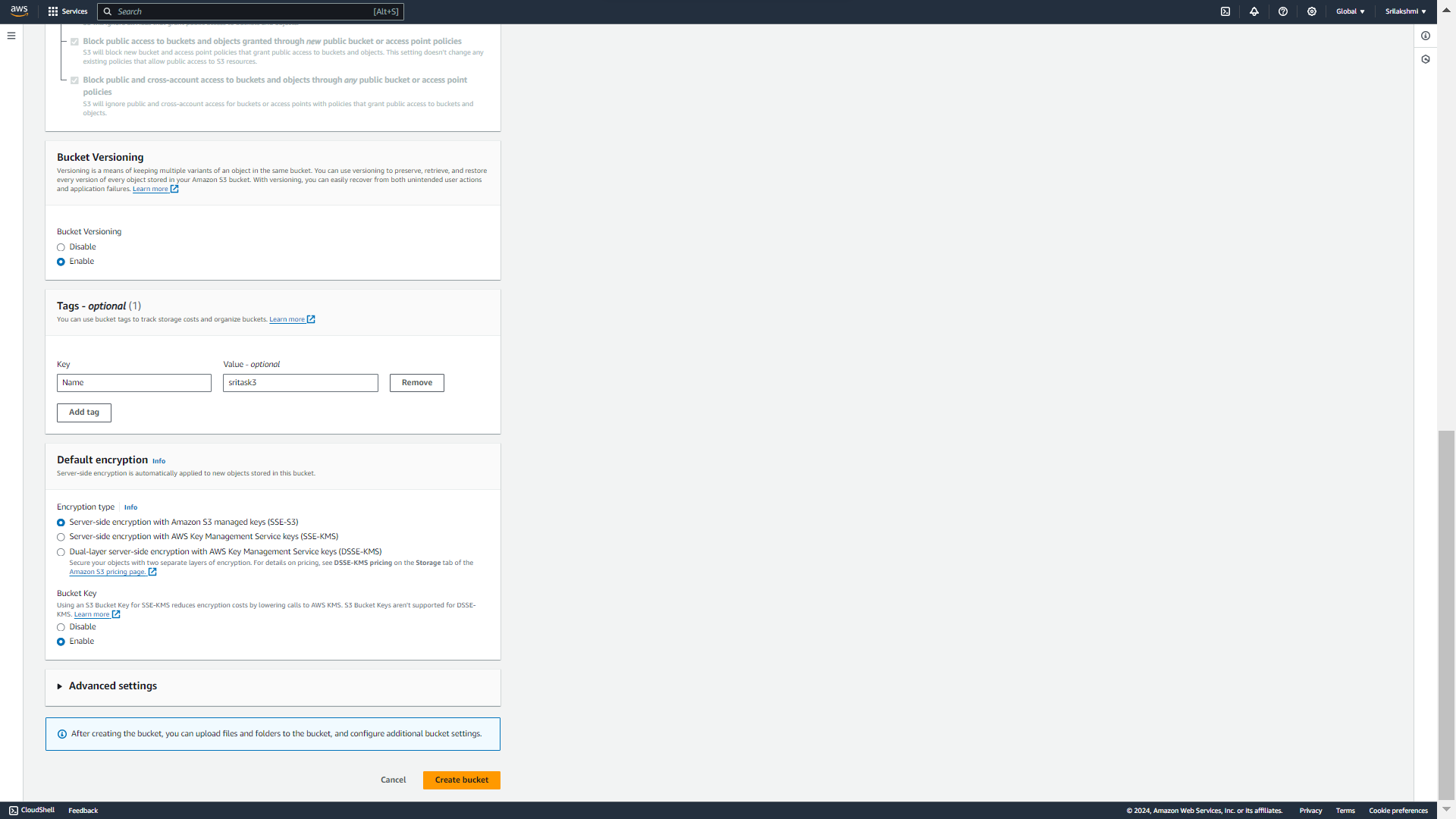
**Select bucket type-general purpose, bucket name-sritask3  
object ownership-ACL disabled  
Whatever data we are creating under this bucket we need to mention some ownership  
By using ACL we can define which persons to allow or restrict the access**



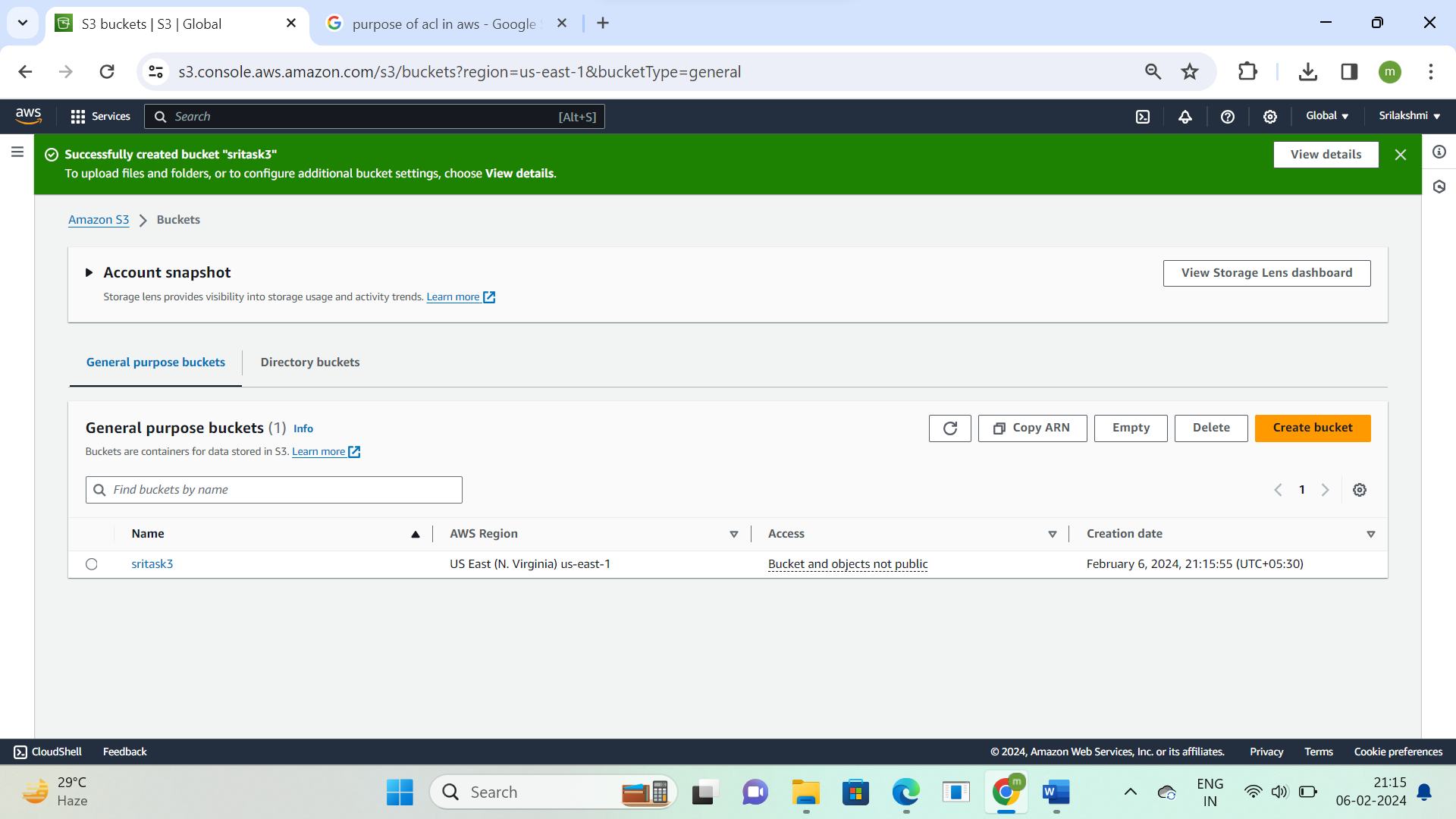
**Block public access**



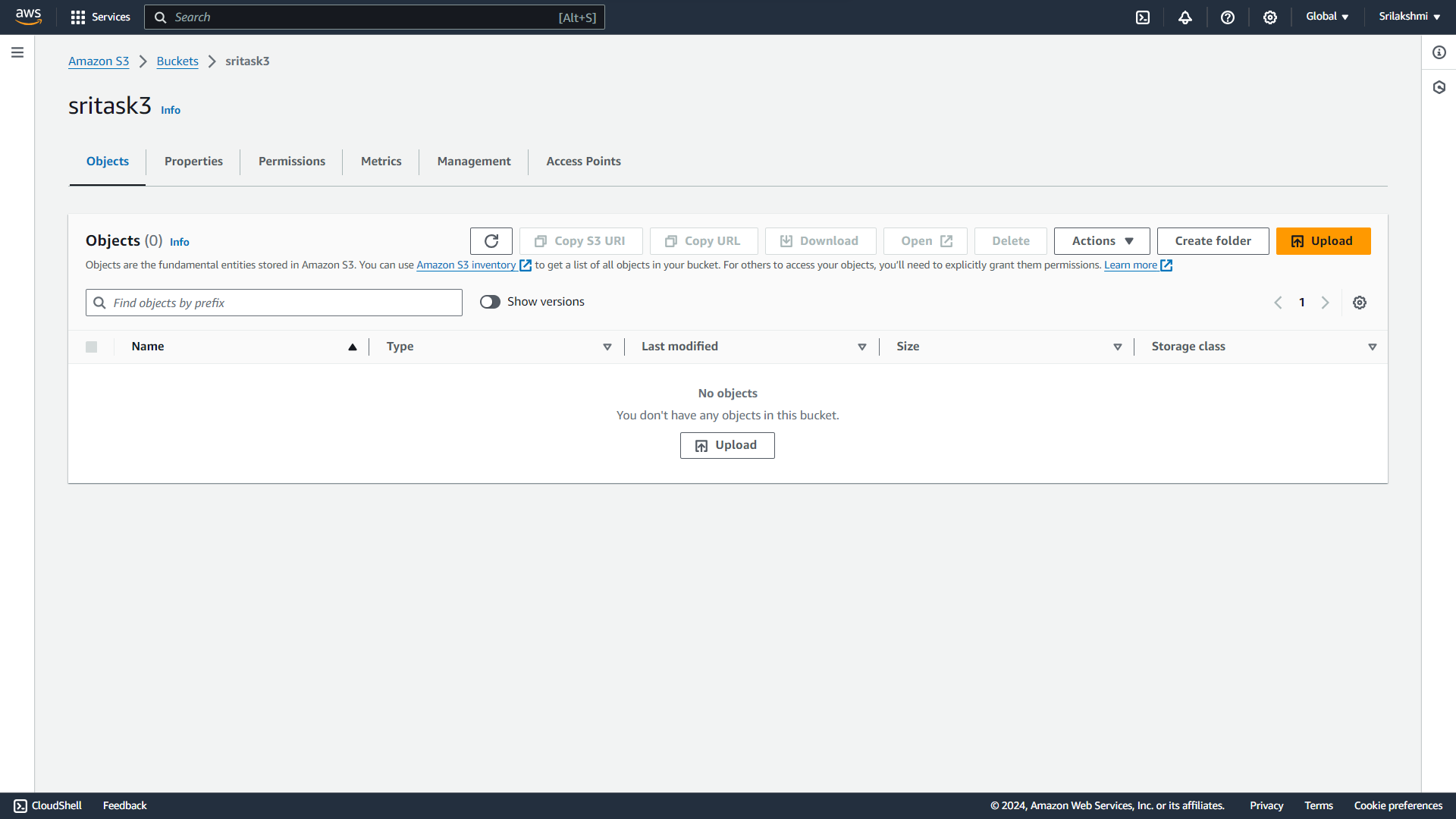
**Enable Versioning, encryption and create bucket  
In versioning we can create, modify and delete data**



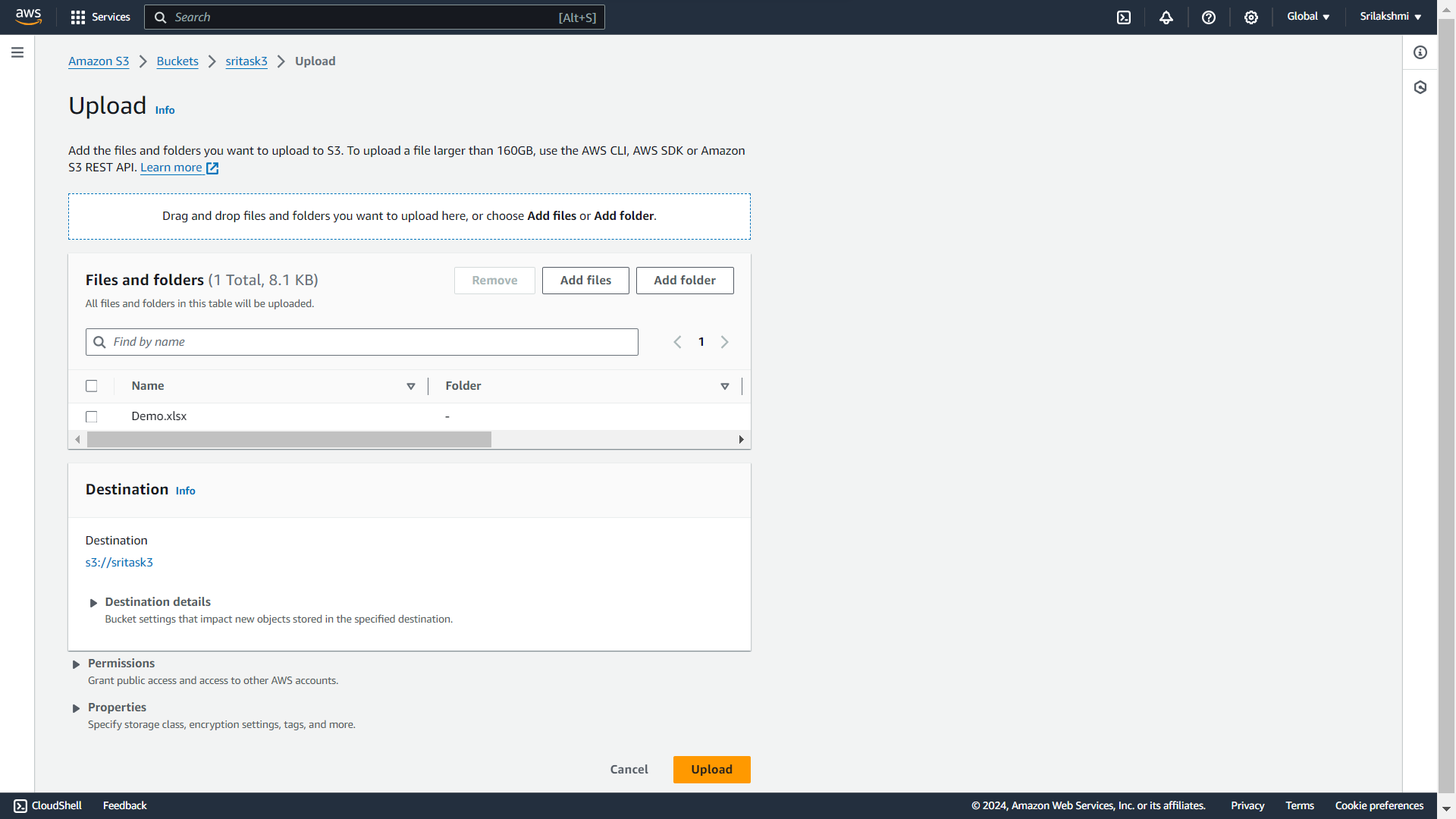
**This is the general purpose S3 bucket-sritask3 click on it**



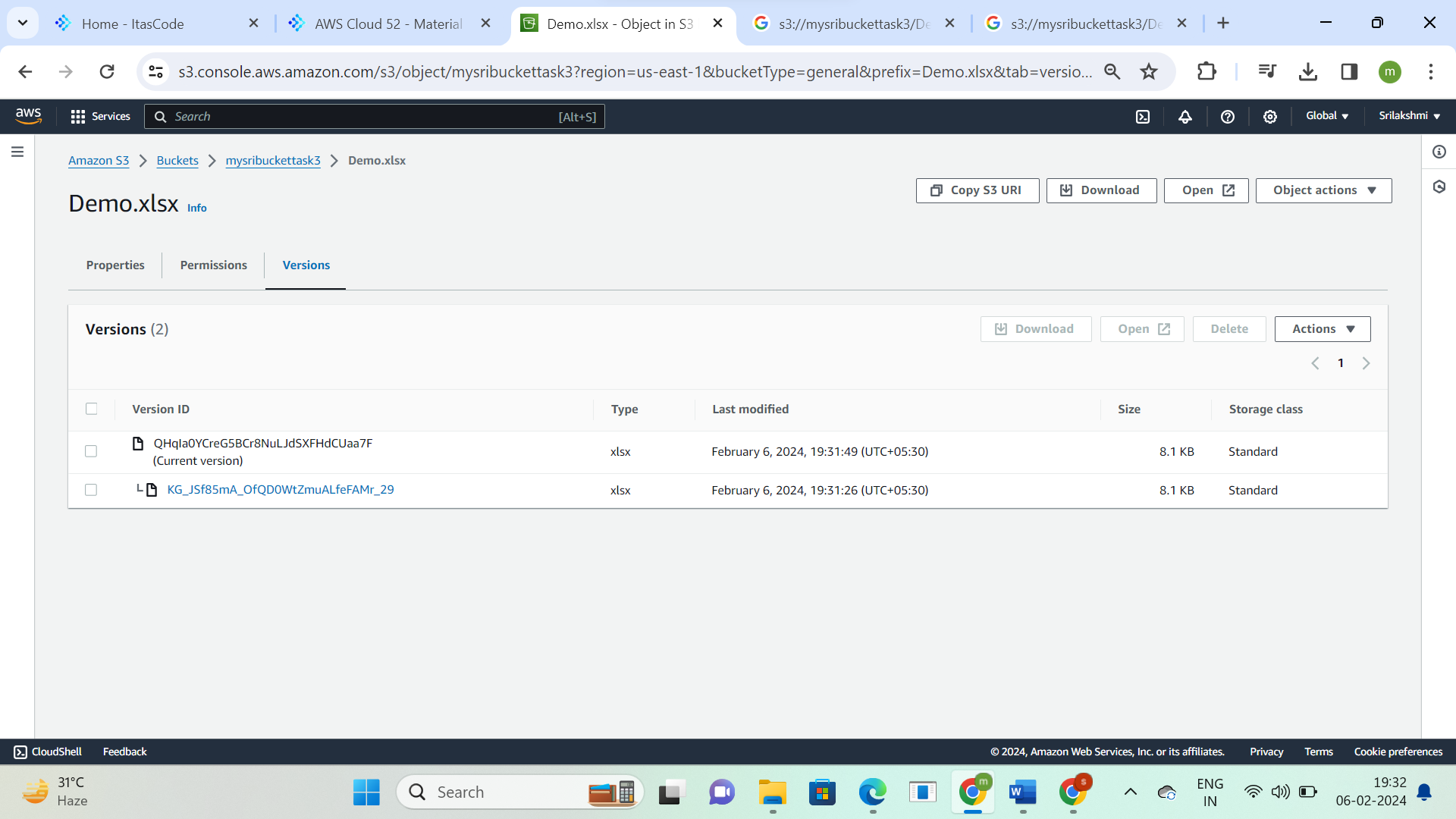
**Click on upload option**



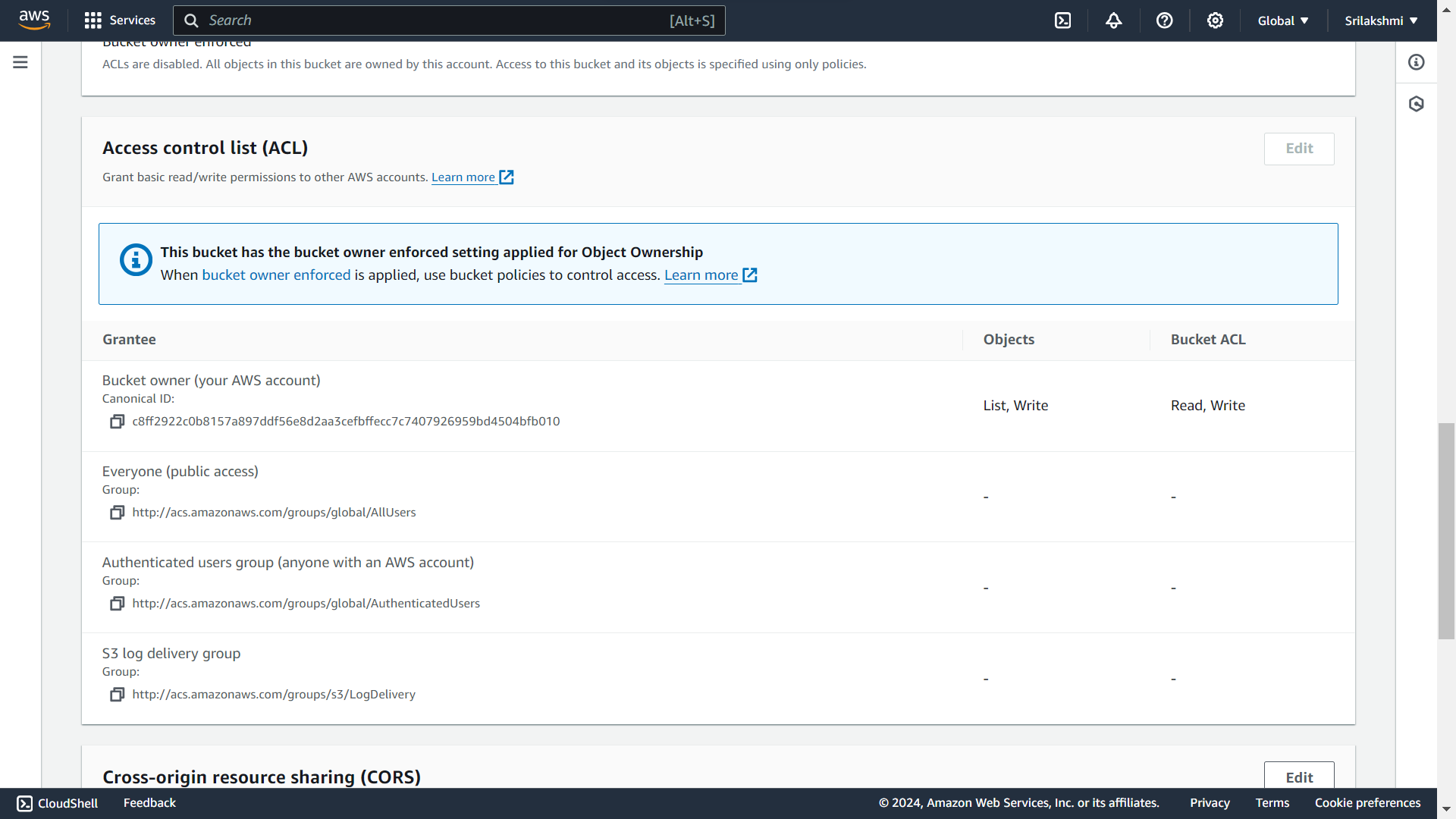
**Add file**



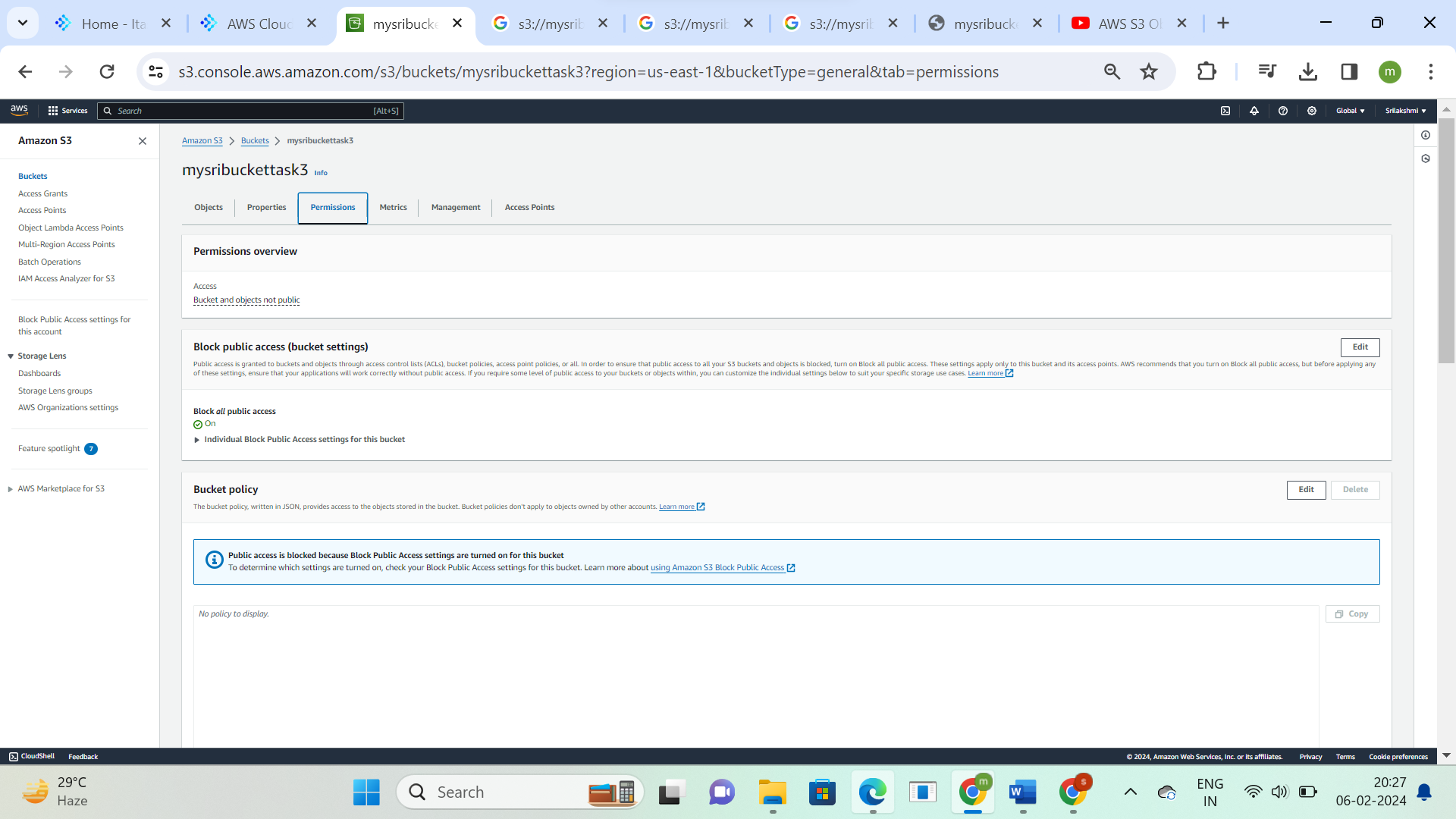
**Uploaded 2 files with same name and different data  
We can add or modify or delete the data in versioning**



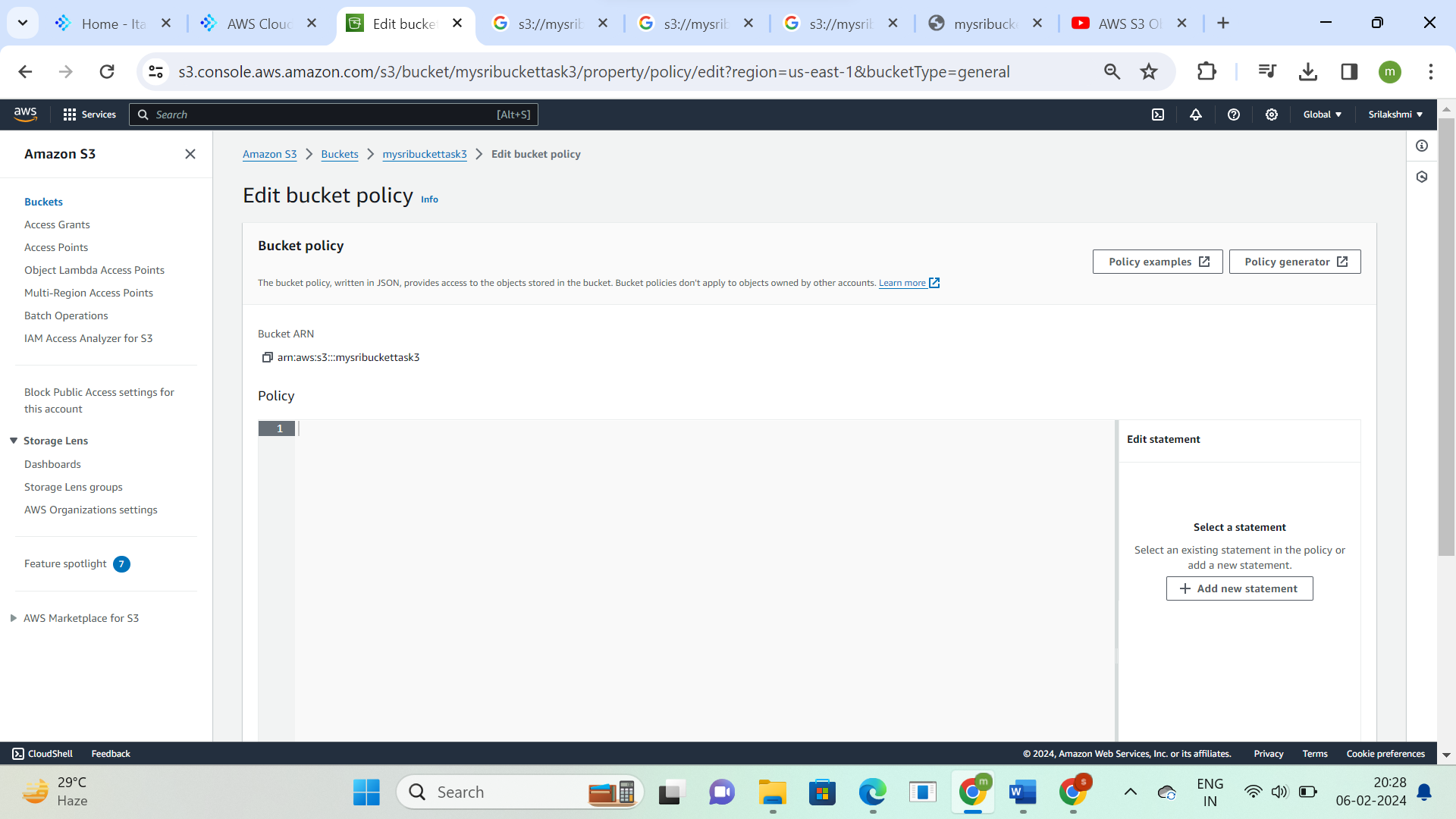
**(Access control list)**



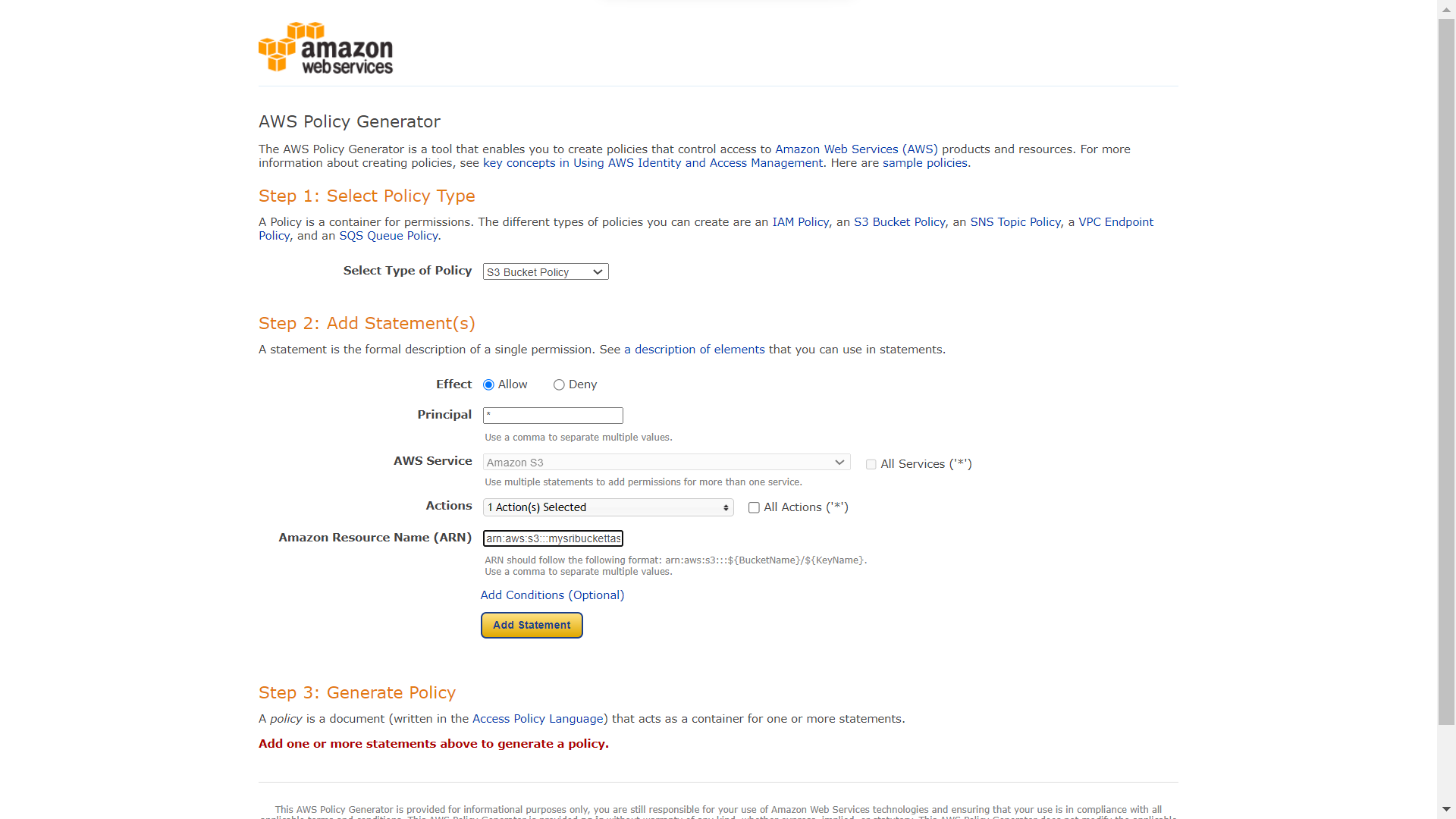
**Go to permissions and click on edit bucket policy**



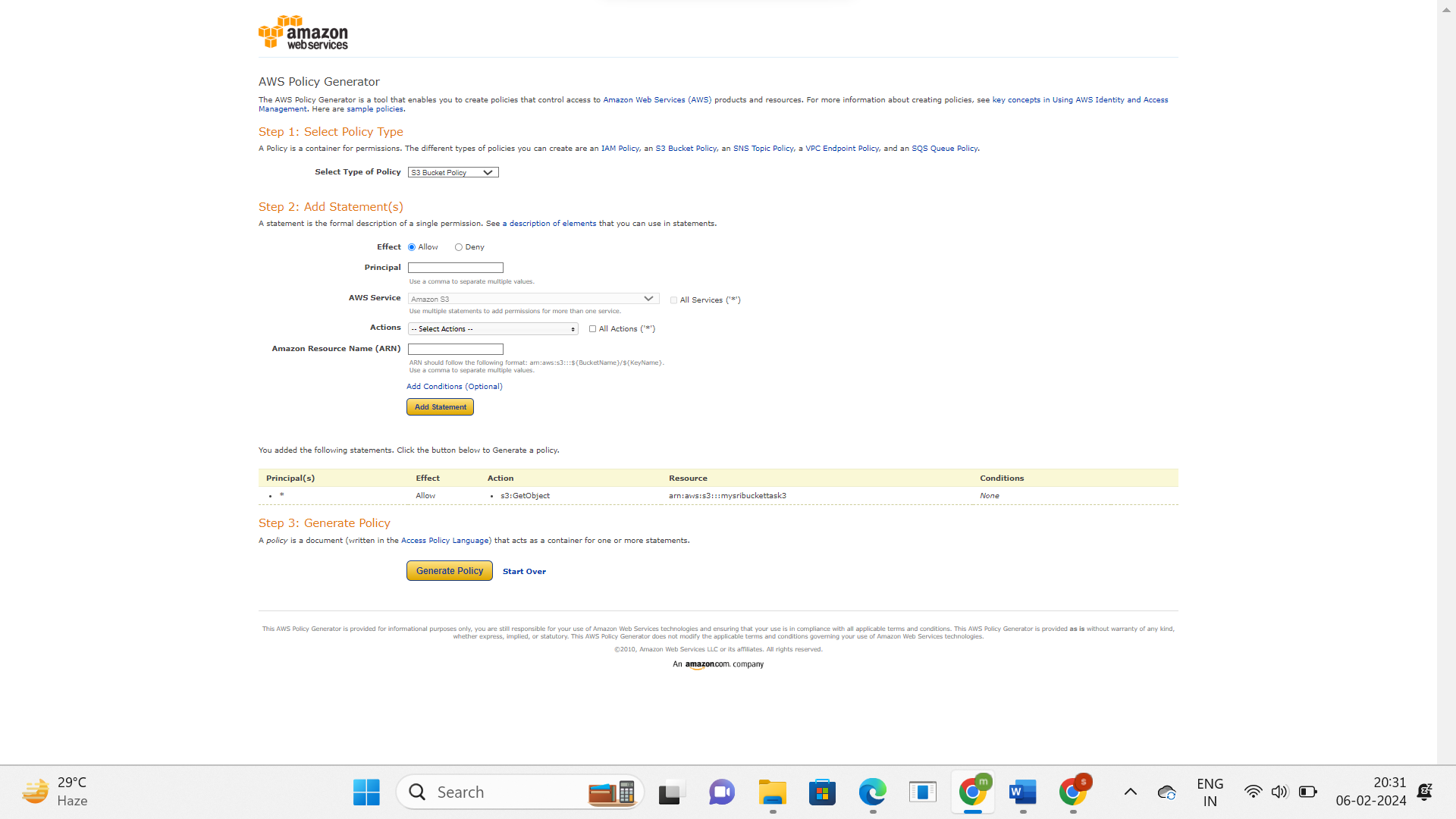
**Click on policy generator**



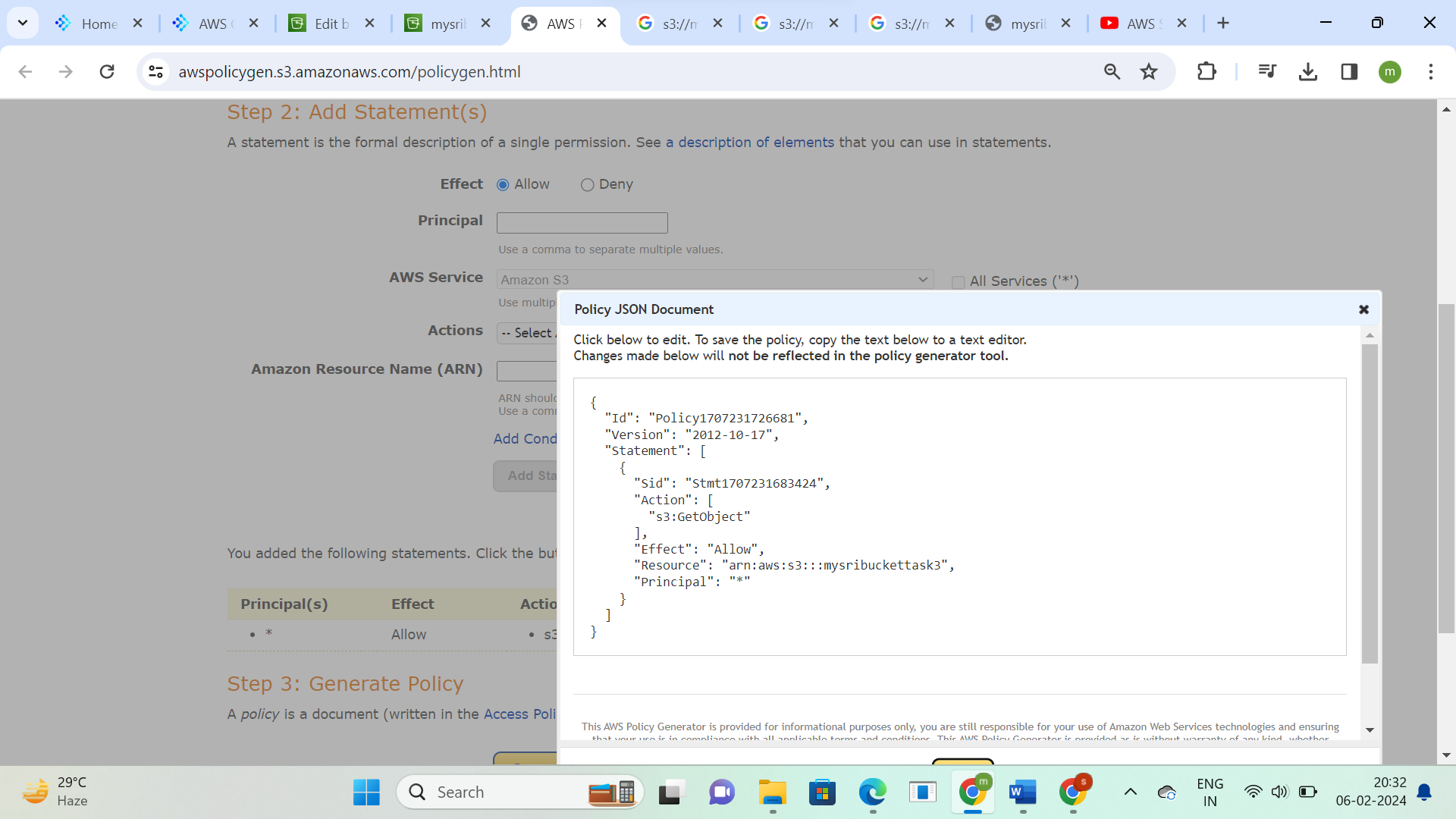
**Give the details and click on add statement**



**Click on generate key**



**Copy the script**



**Paste the script in the policy and click on save changes**

