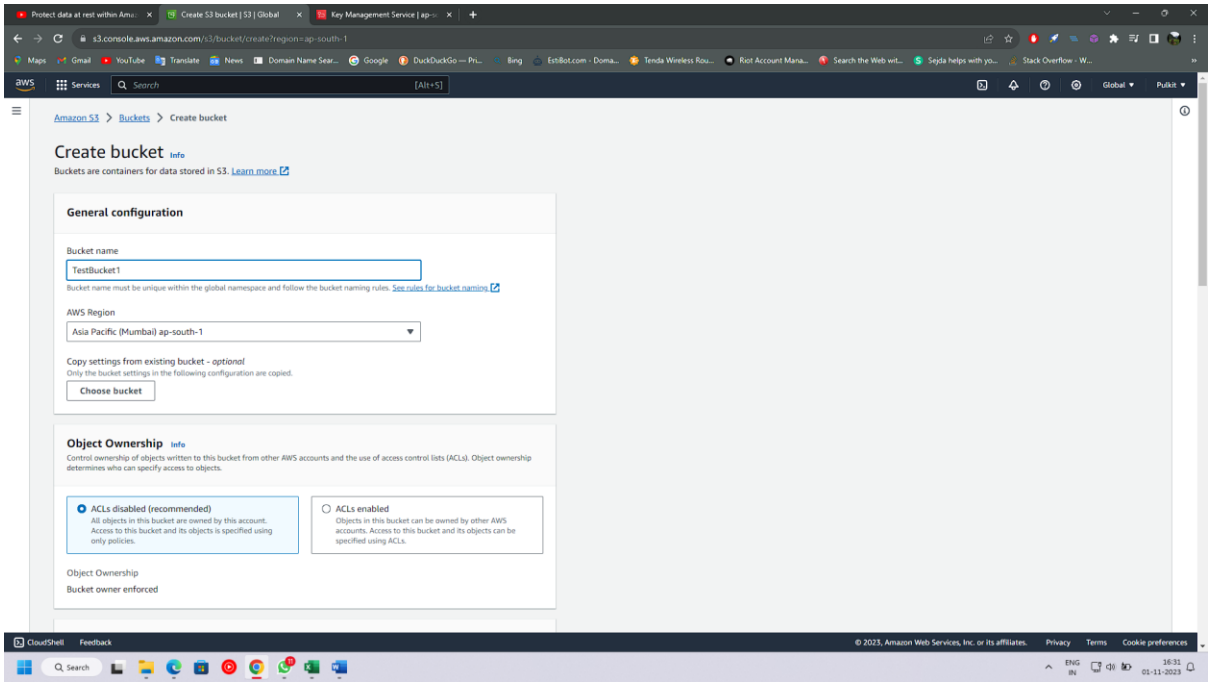
😊 Protect data at rest within Amazon S3 data centres by using AWS KMS

STEP 1:

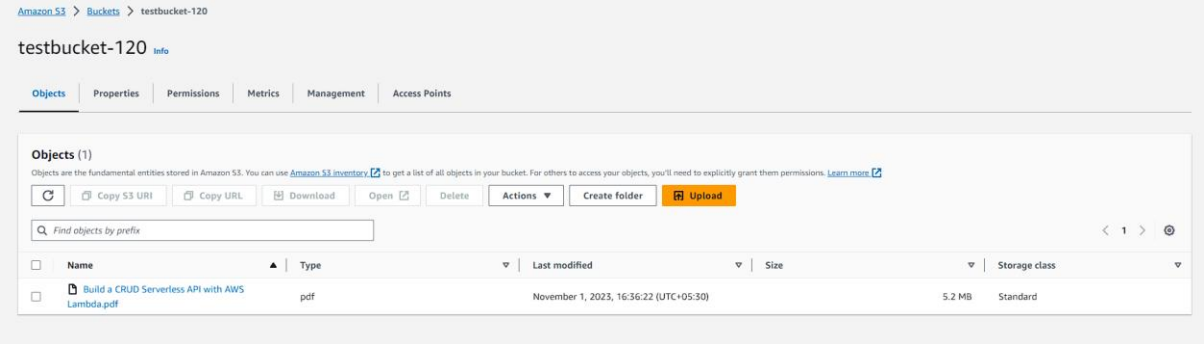
1. Log in to Console
2. Then go to IAM and Create a Root user (We can use existing user as well) and give it a permission for S3 read only.
3. Then log into the Root user using a different browser.

STEP 2:

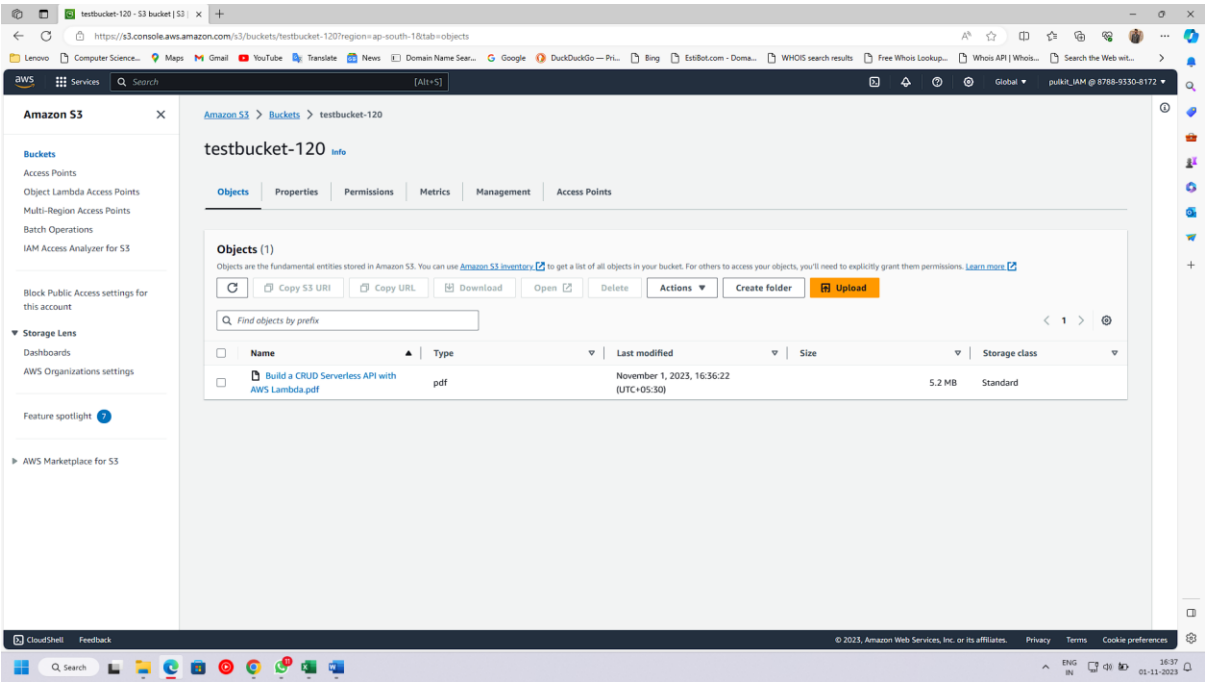
1. Create a S3 bucket in main account and keep the settings to default.

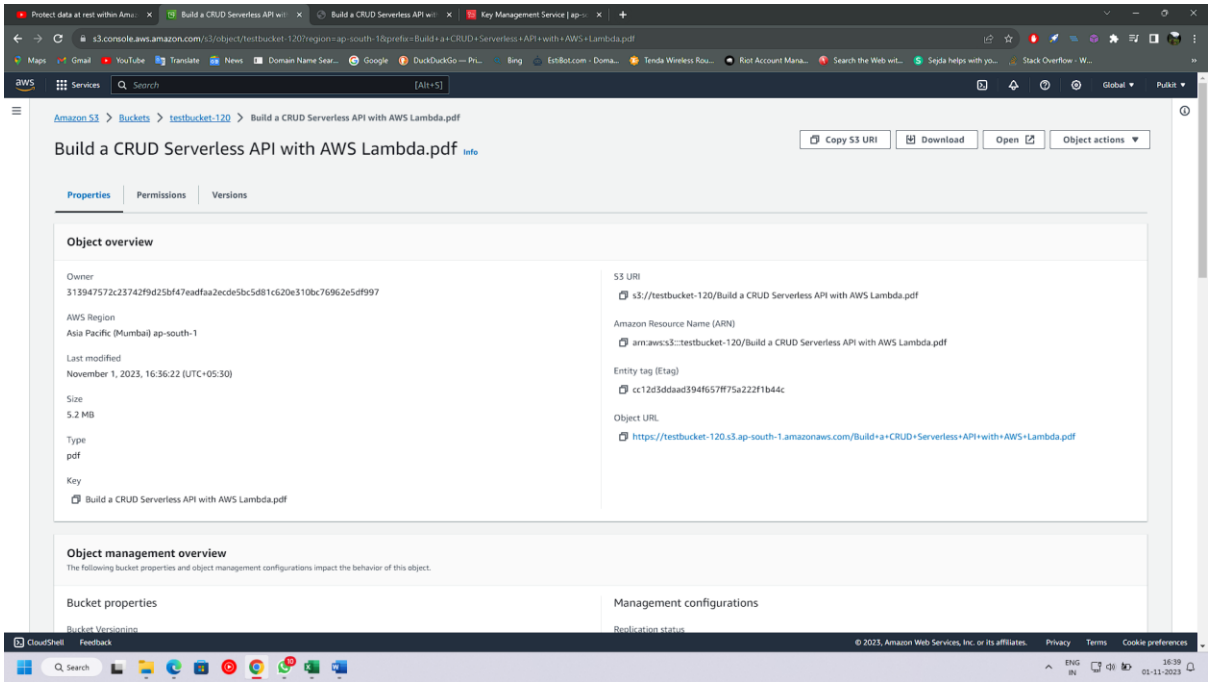


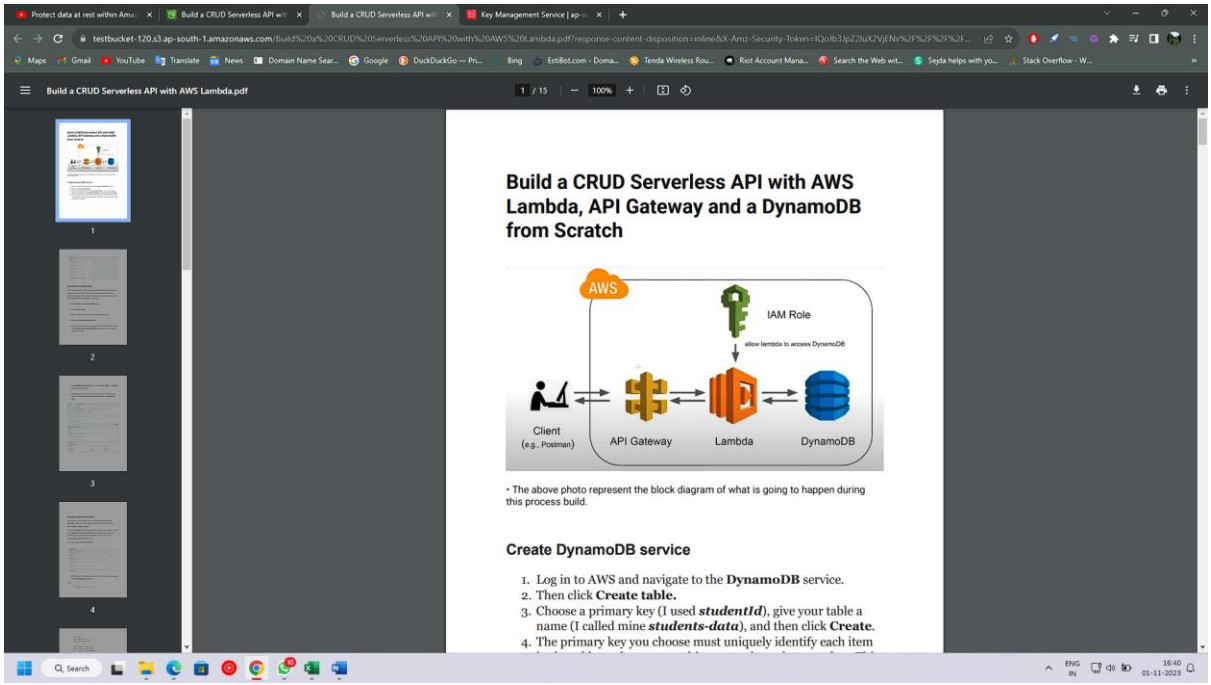
2. Go to Root account and open S3 in it too. We'll see the same bucket that we created in main account.
3. Now go back to main account and upload a file to S3 bucket from our system. And we'll see the file in the bucket.



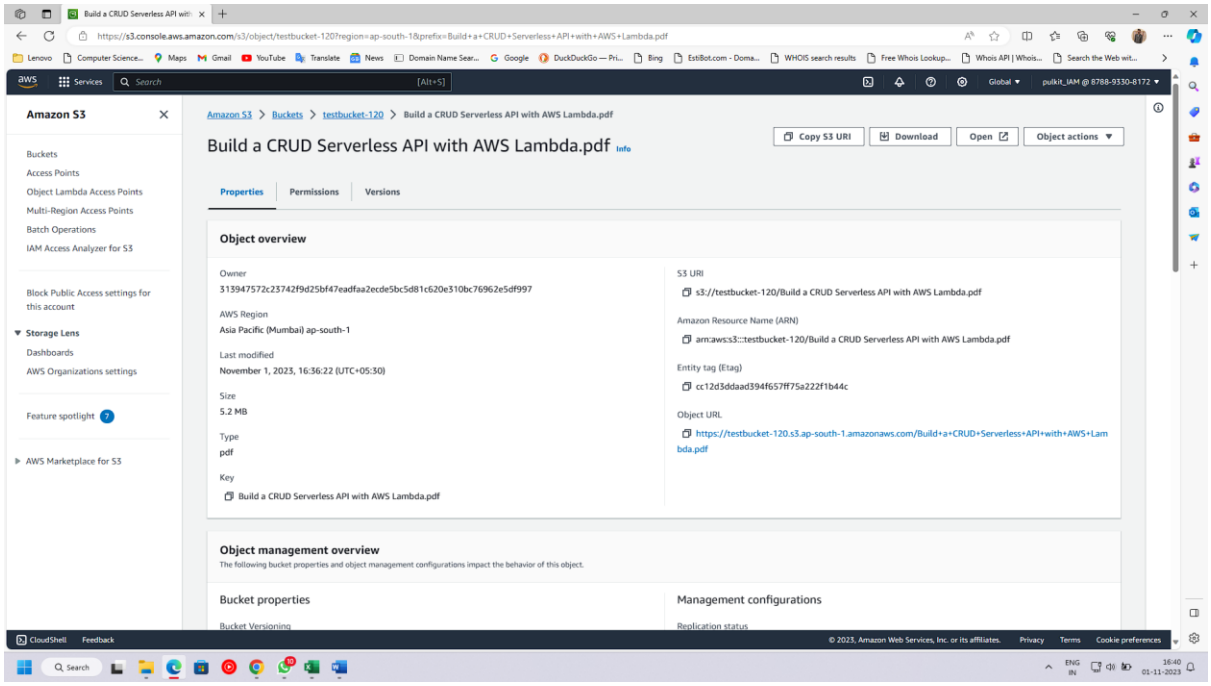
4. And if we go to the Root user we'll find the same file in it. If we want to open it we can see the content in the file present.

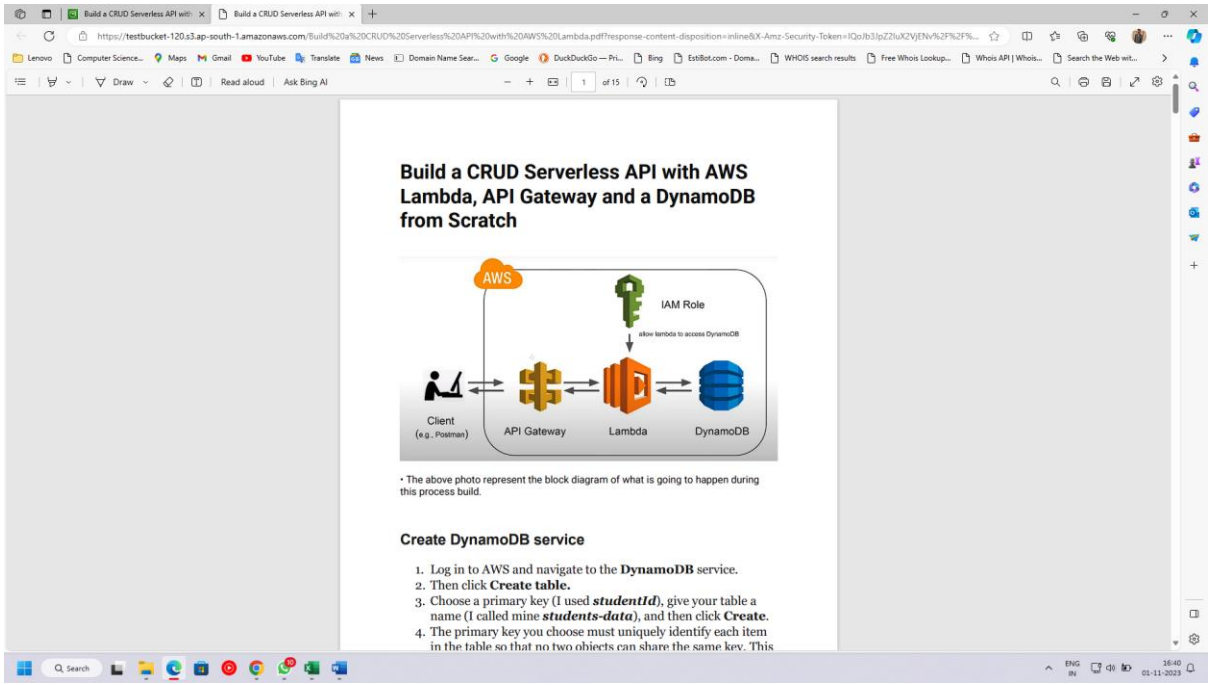






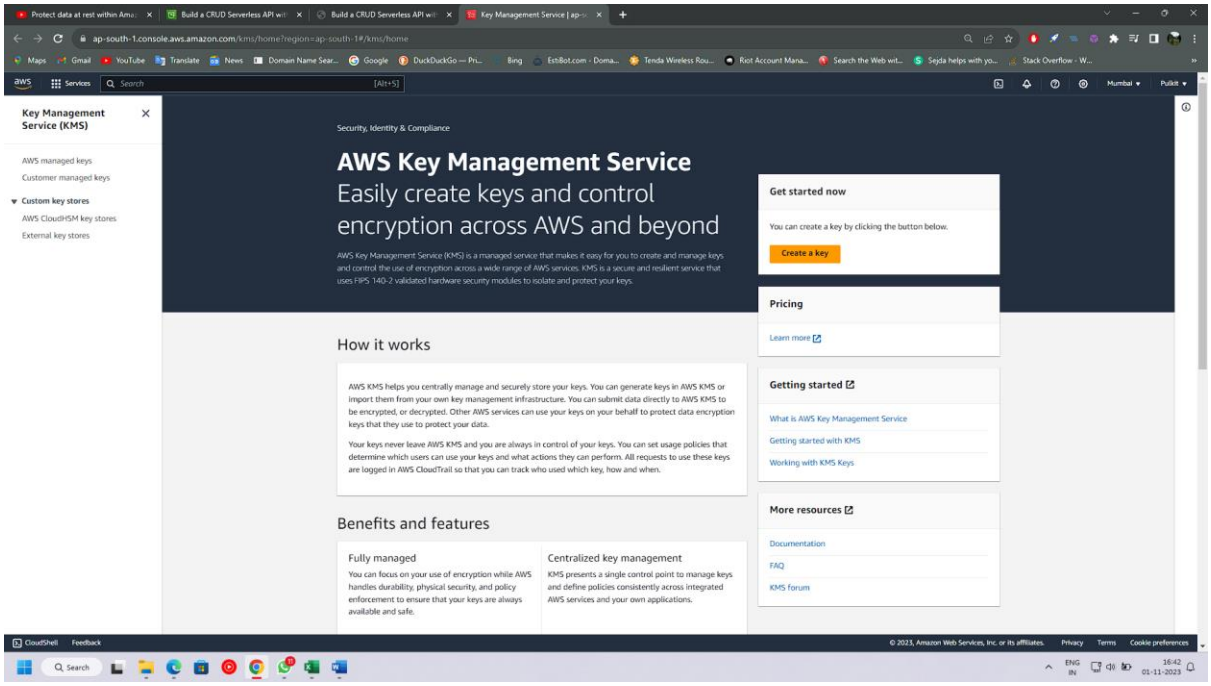
5. And if we go back to Root user we can do the same in it too.

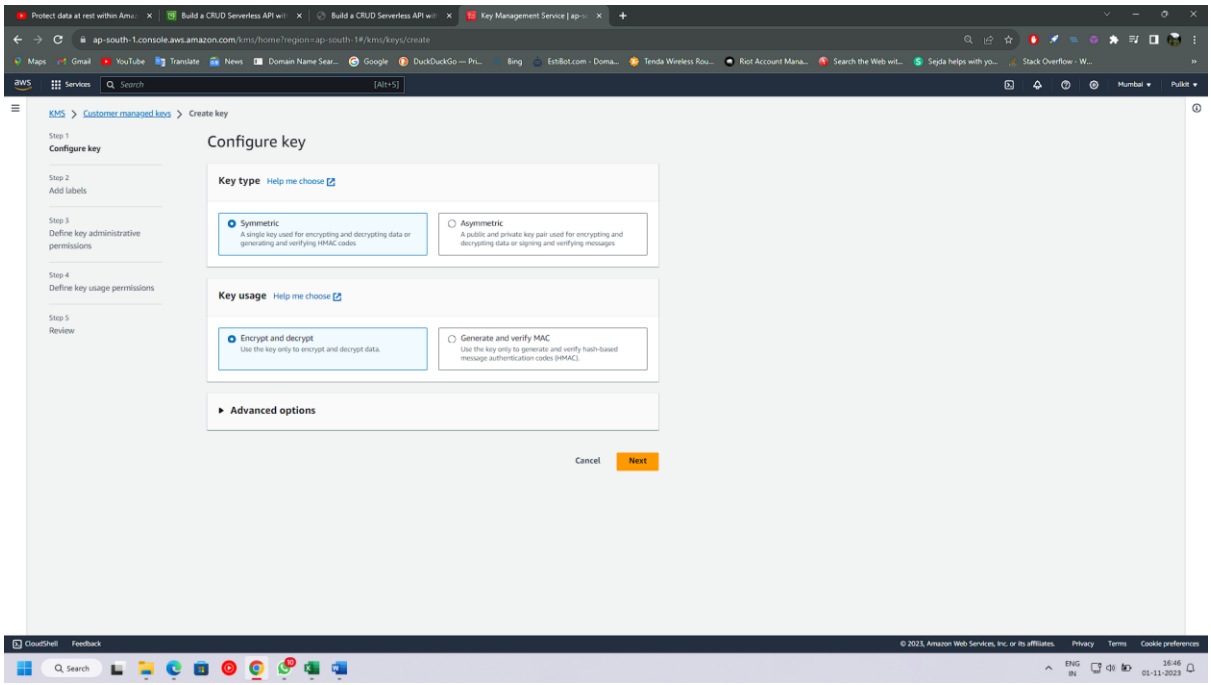




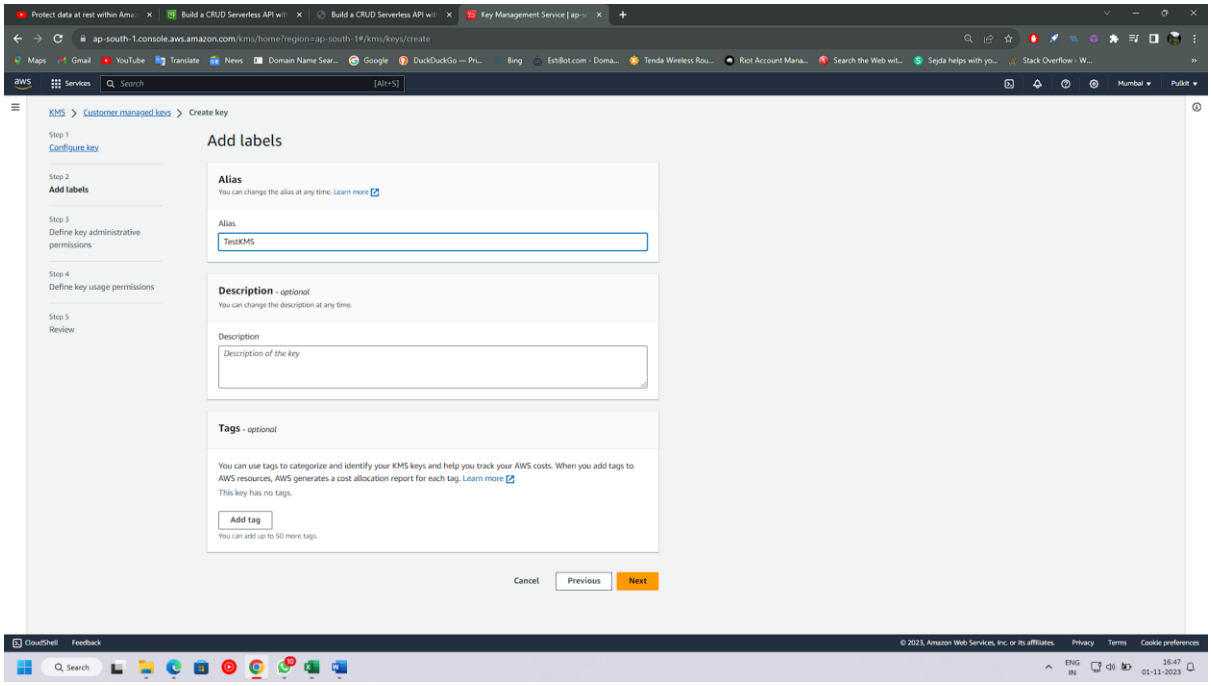
STEP 3:

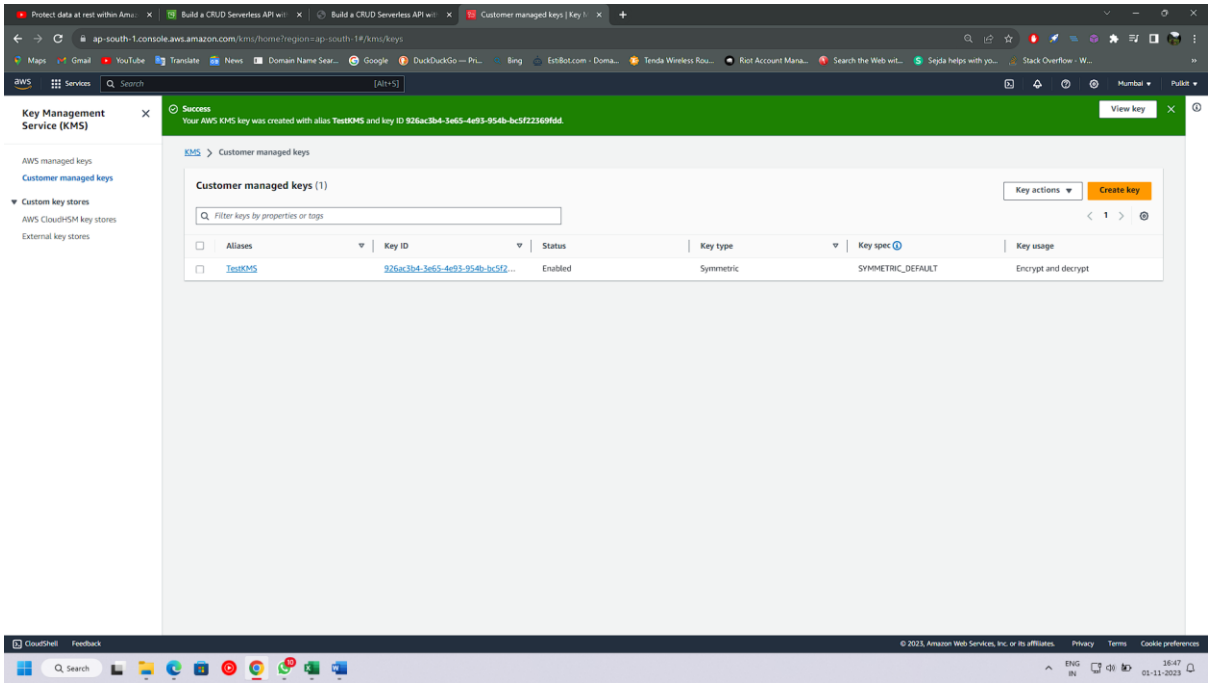
1. Now go back to main user and search Key Management Service (KMS) and create a key to secure our file in S3.



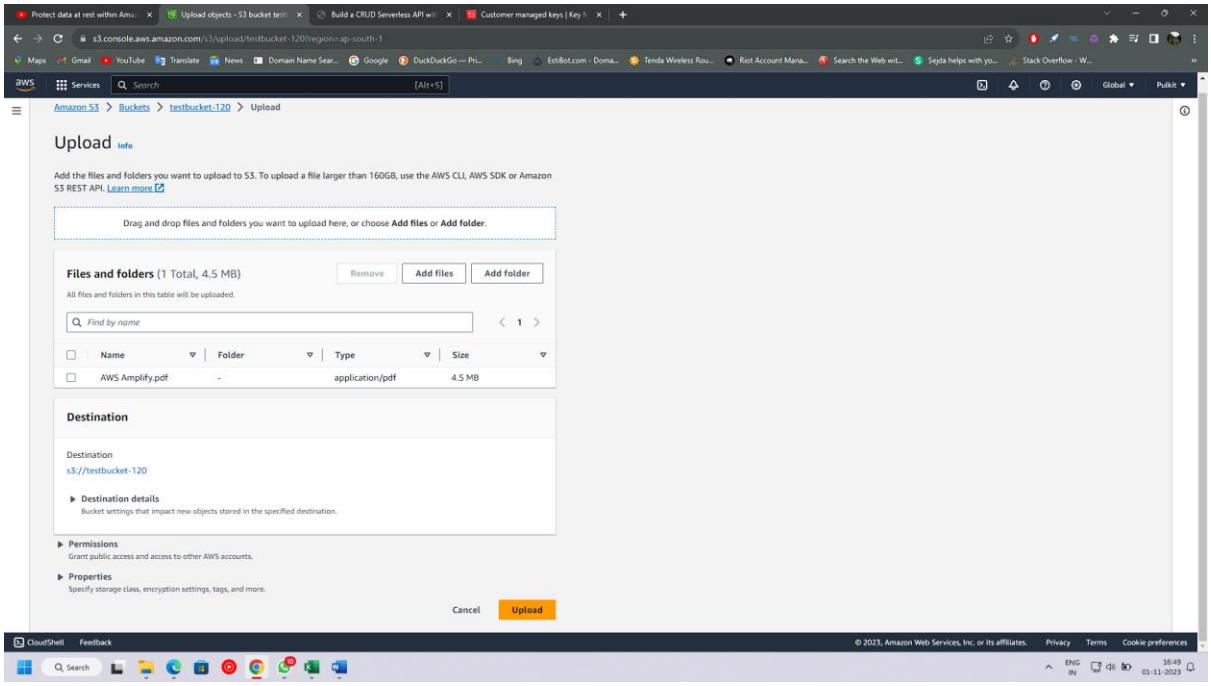


2. Just give it a name then keep everything default and create a KMS.

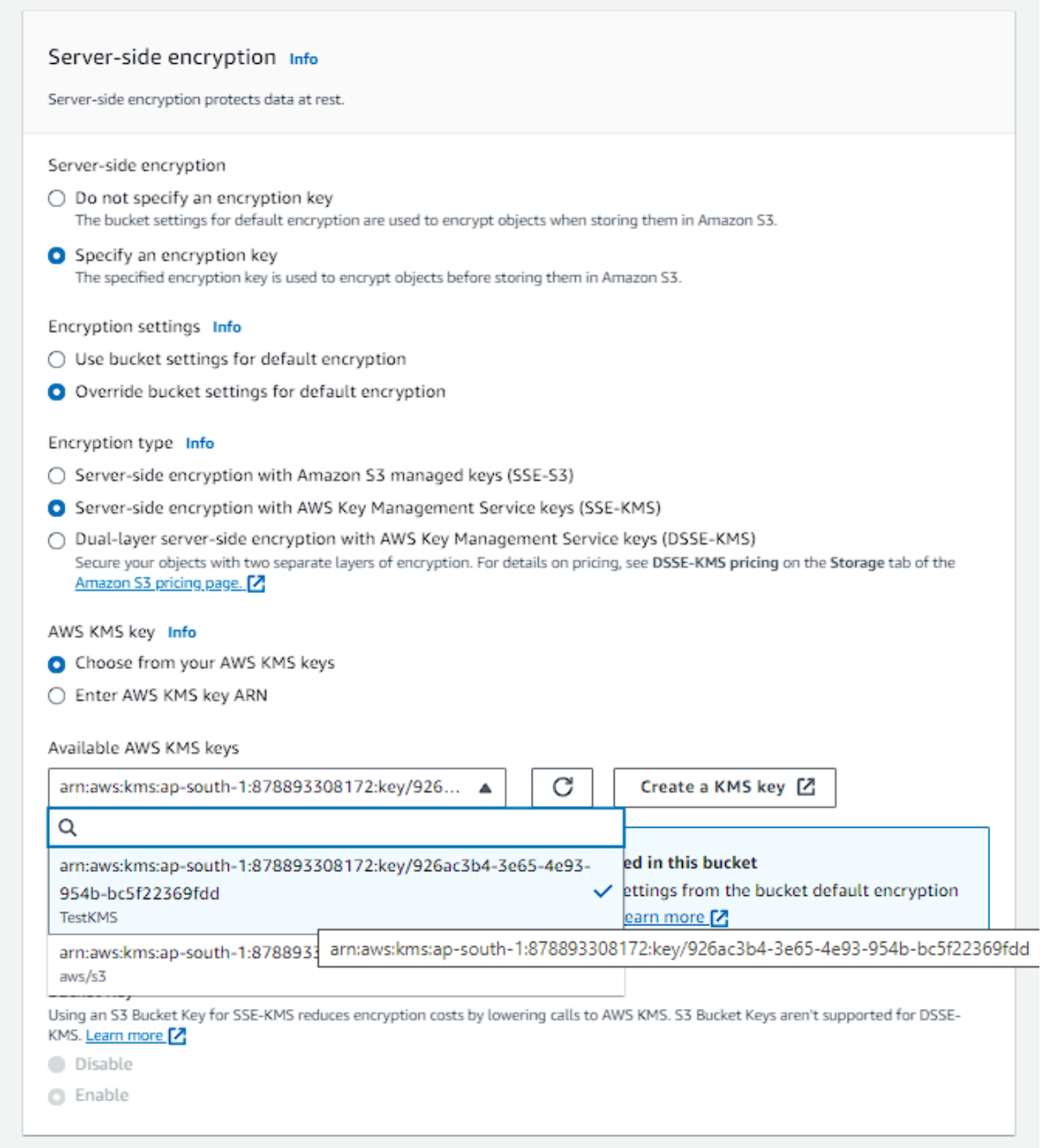




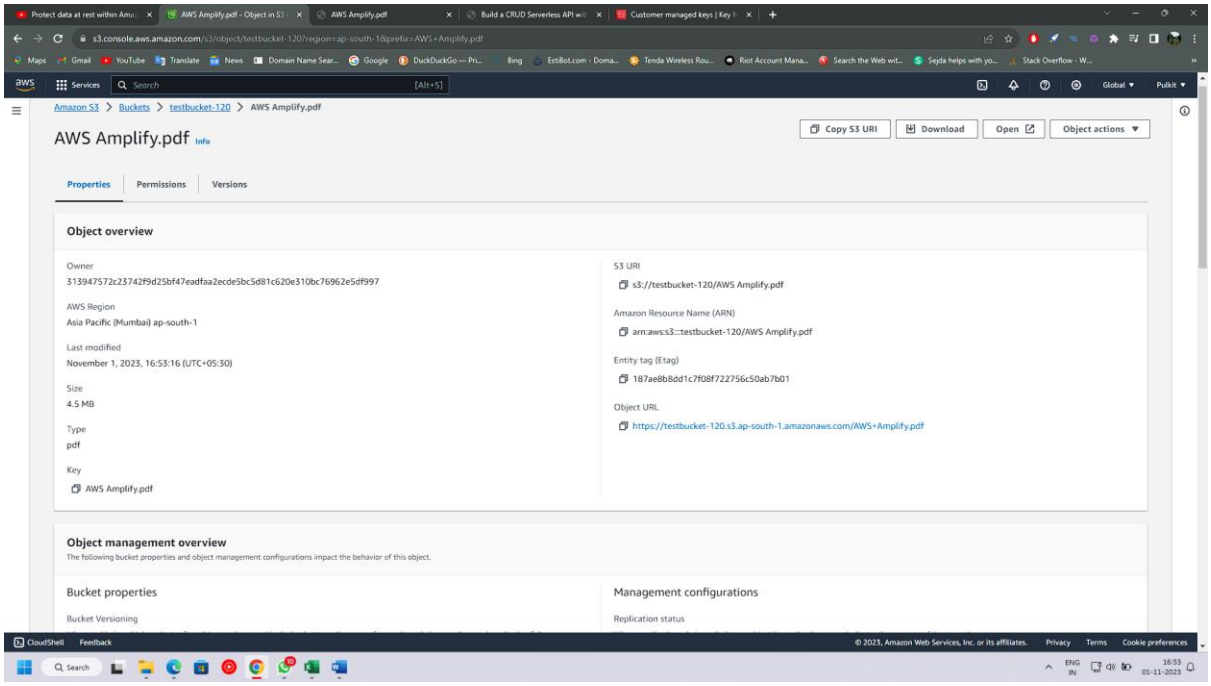
3. Afterwards go back to S3 and upload another file.
4. Once we've uploaded the file we'll see Properties option at the last click on it.

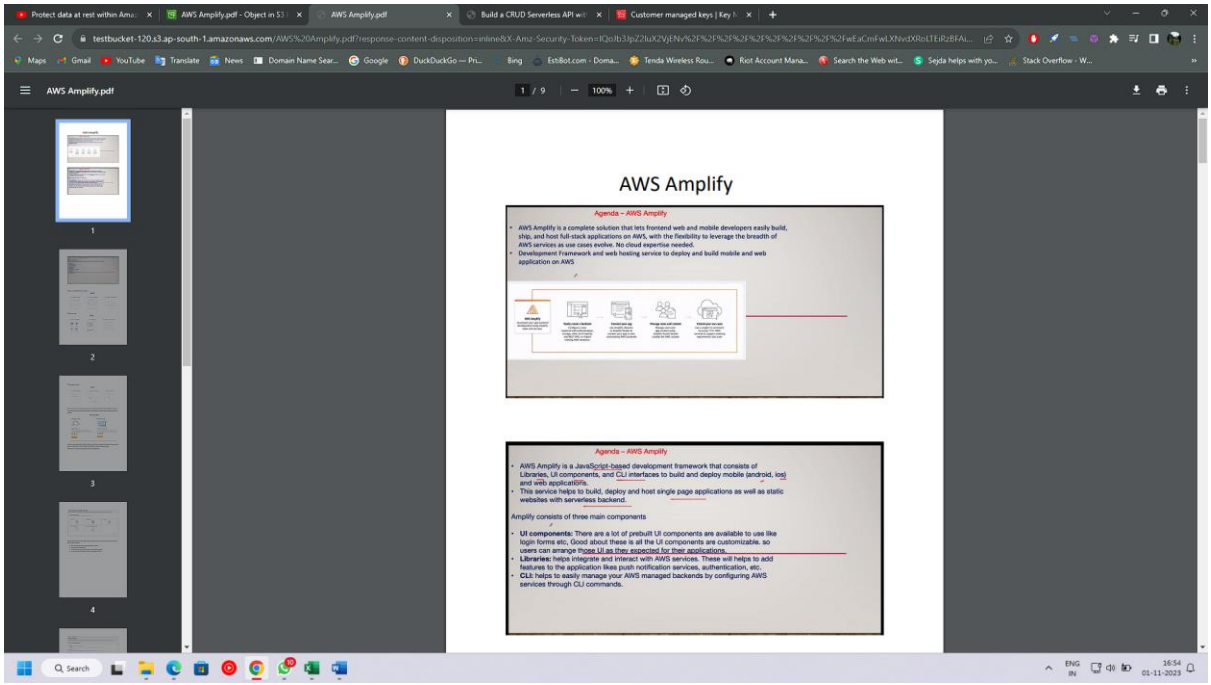


5. Then scroll down a little and we'll see a option named Server-Side Encryption and on it choose the option below. (And choose the KMS which we created earlier)
6. Then click on upload.

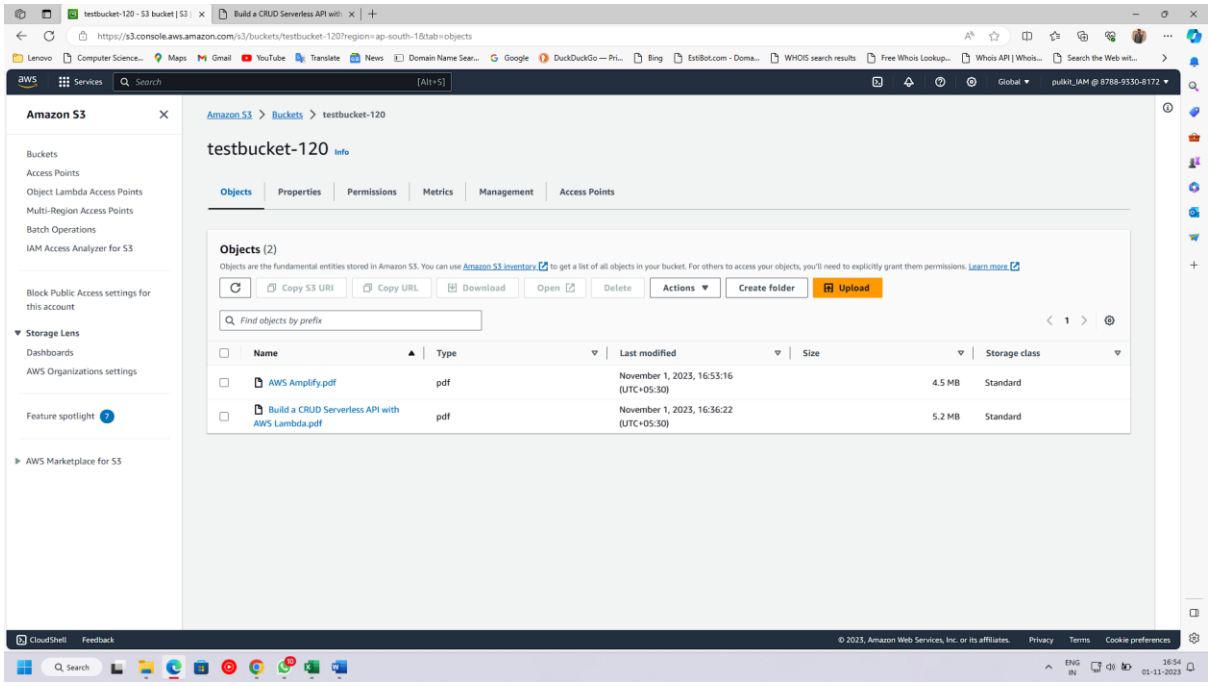


7. Now if we open it from our main account it'll get open and it is readable.

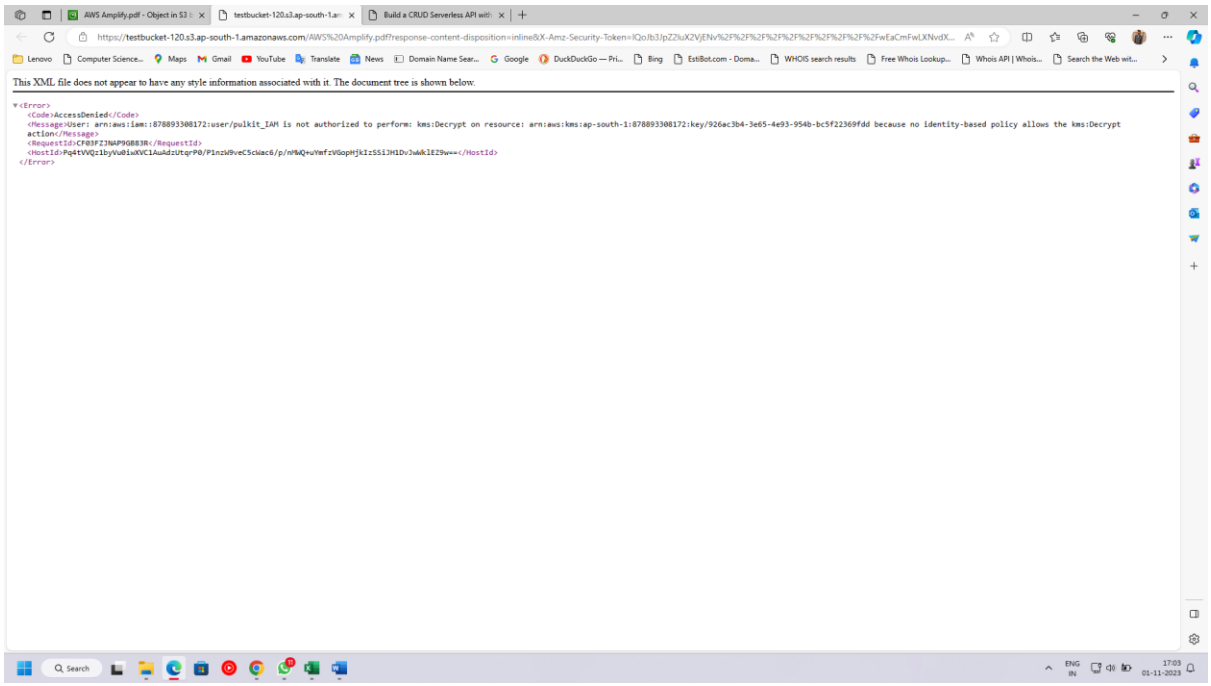




8. Now if we go to our Root Account we'll see the same in it too.



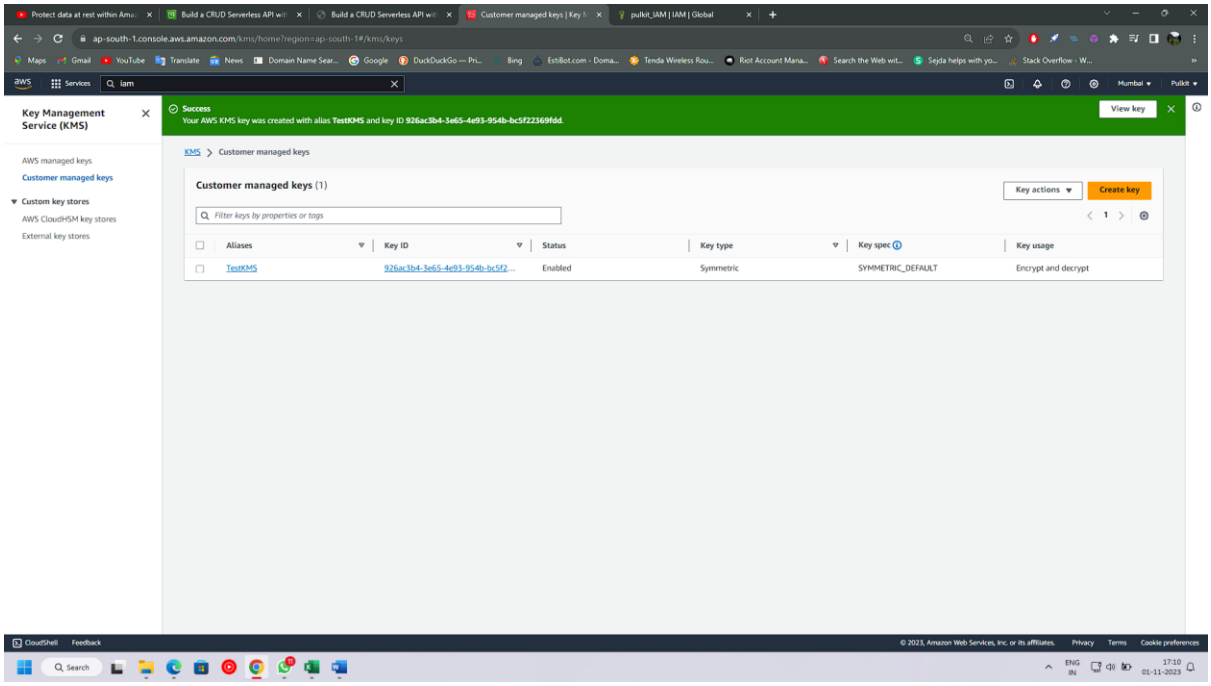
9. But if we try to open this file then we'll get this message (Access Denied) which means that our file is secured.



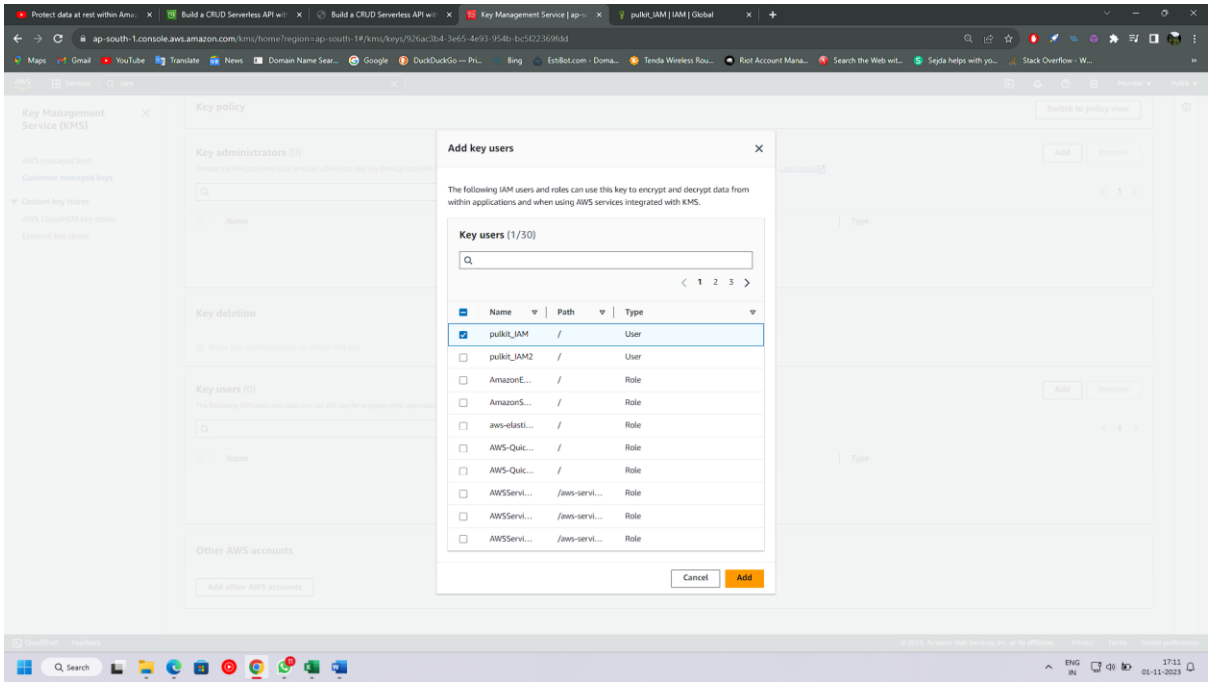
10. This is how we secure our file.

LAST STEP:

1. If we want to give permission to the root user to access that file which we've secured.
2. Then we need to go back to KMS and select the user which we created.



3. Open it and scroll to down to a option which says Key User and select the root user and add it.



4. Now if we go back to Root User and open that same file again then we'll see that we're able to read the contents of that file.