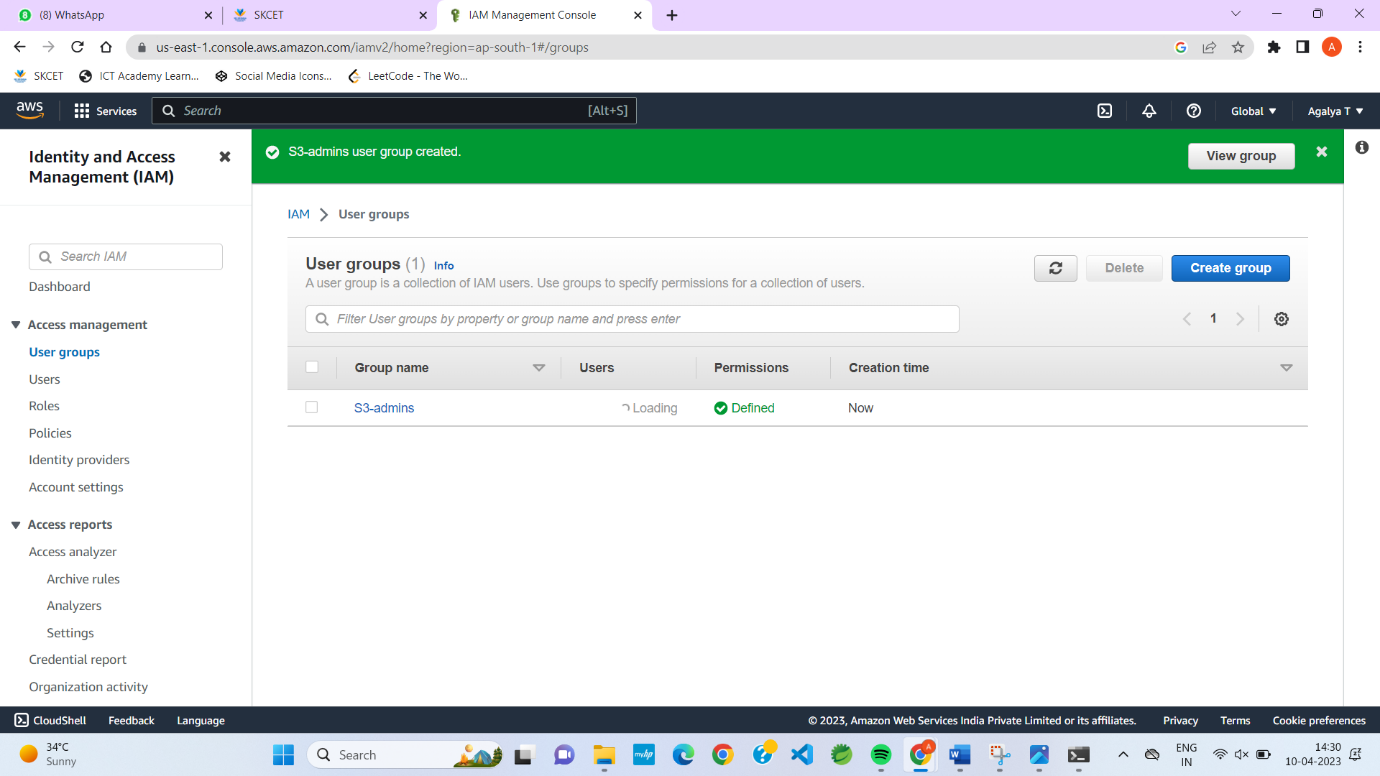
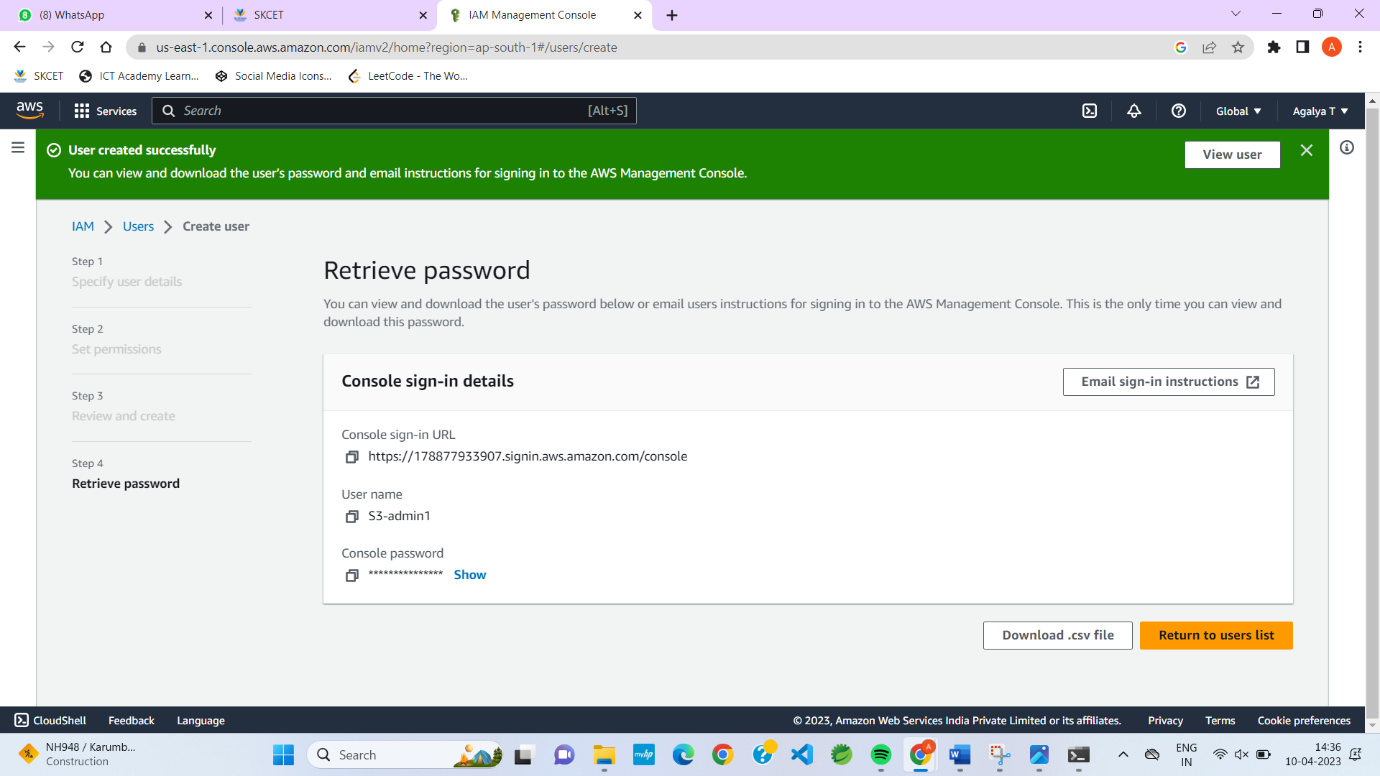
DAY-4

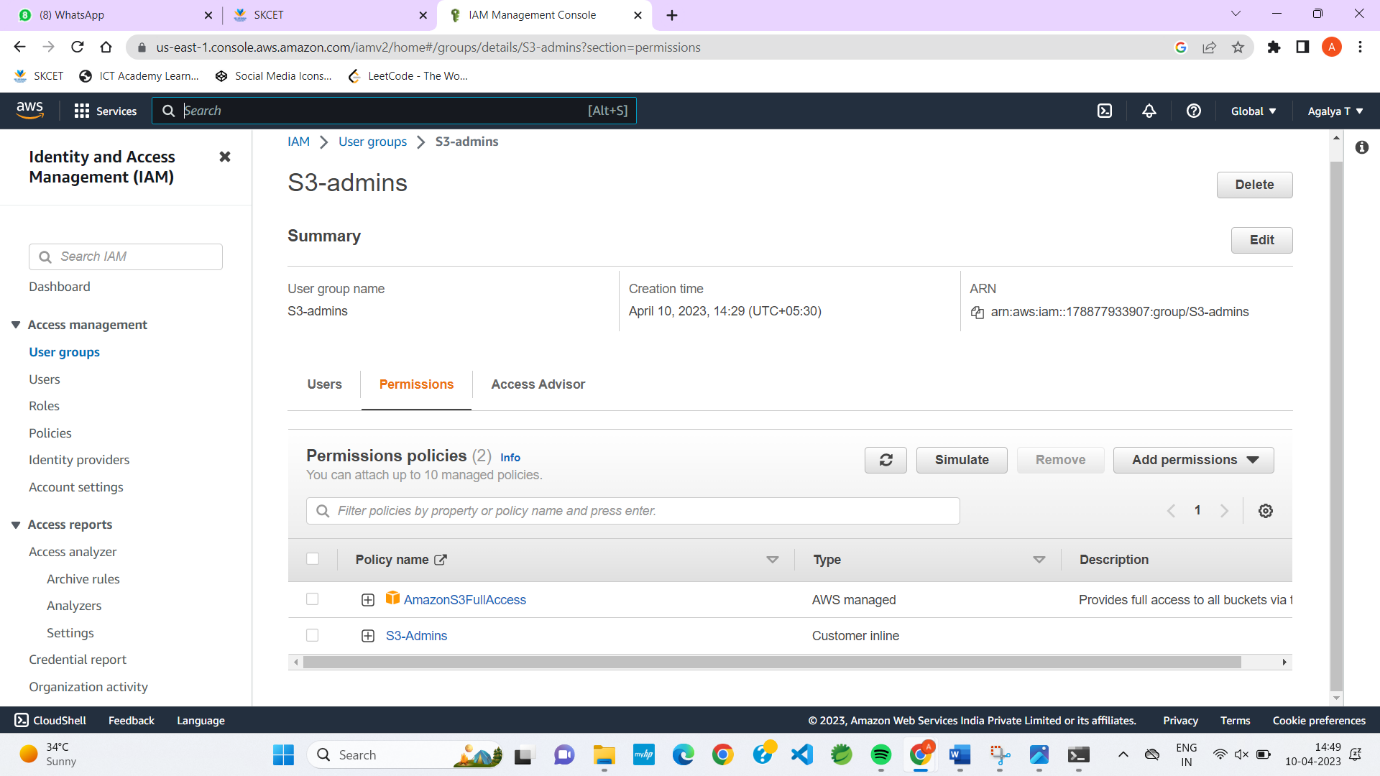
1) Create an IAM group called as ‘S3-Admins’ with ‘AmazonS3FullAccess’.



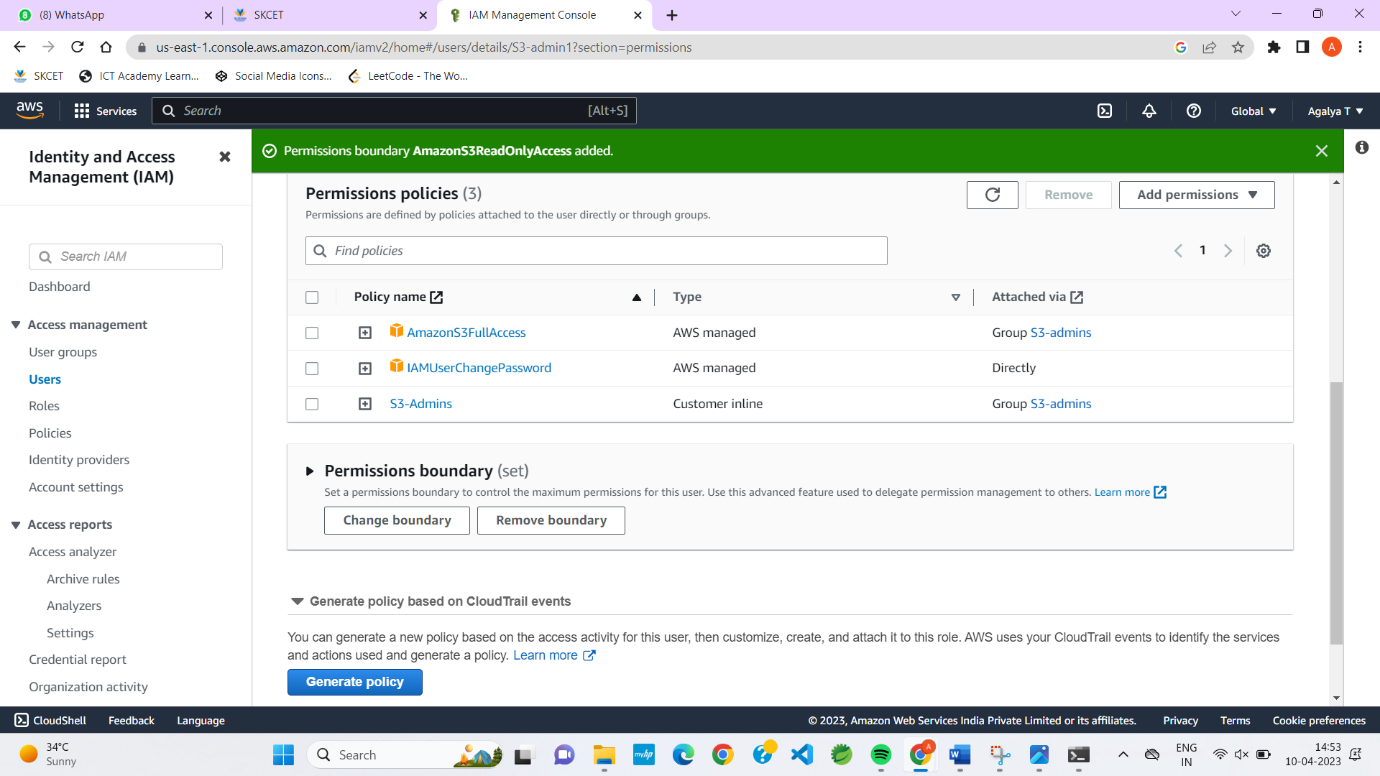
2) Create an IAM user called as ‘S3Admin1’ and add it to the ‘S3-Admins’ group.



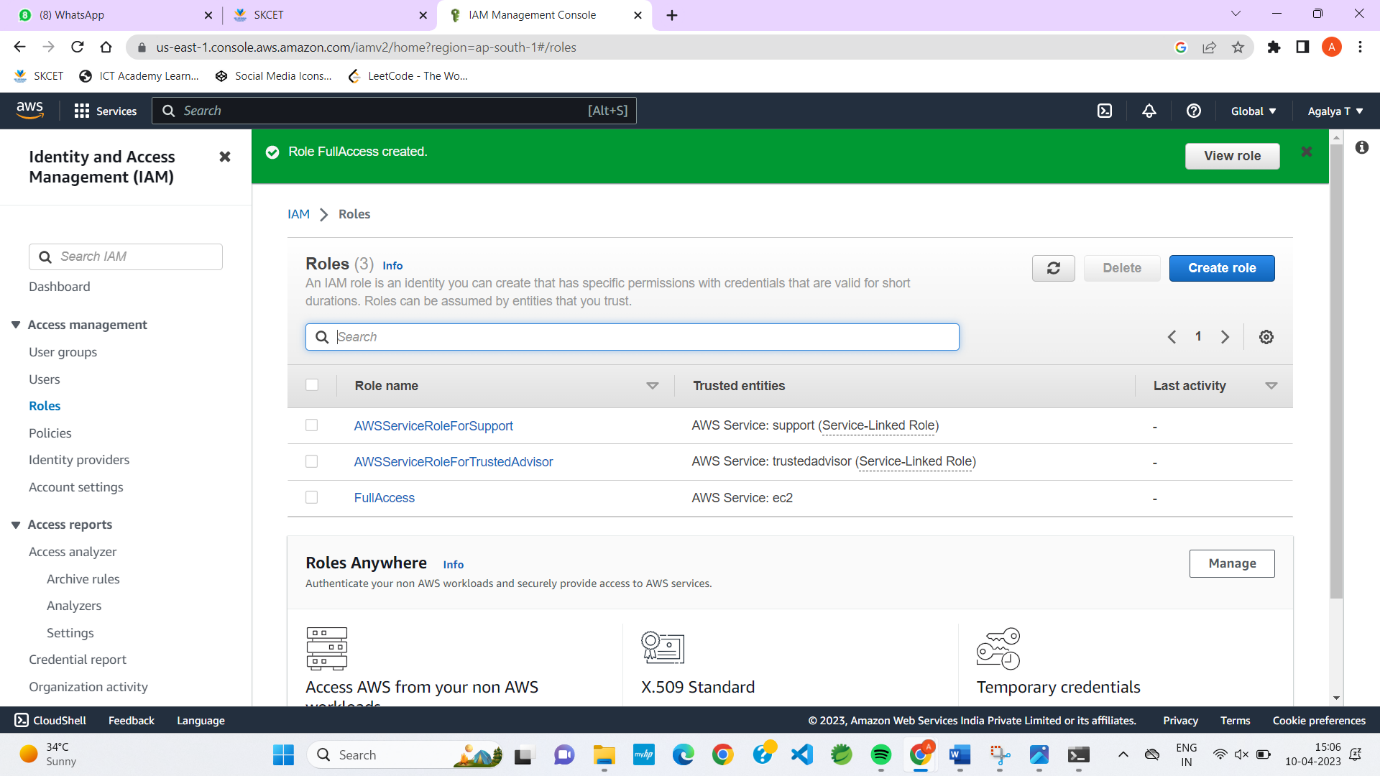
3) Attach an IAM custom policy to the ‘S3-Admins’ group which should deny to delete objects.

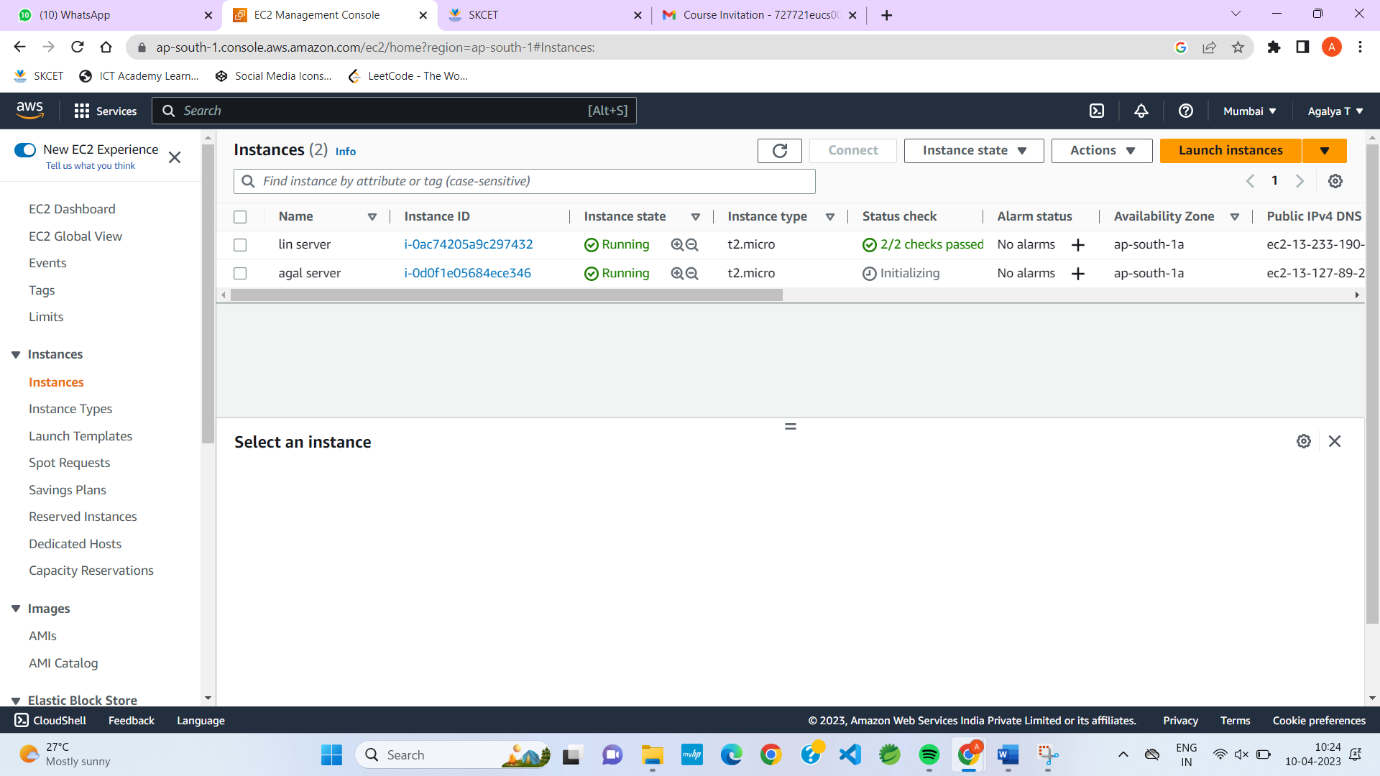


4) Create an Inline policy for an IAM user and set some permission boundary for that user.



5) Create an IAM role with ‘AmazonS3FullAccess’ and attach the role to an EC2 instance.





6) Activate MFA for an IAM user and Set some Password Policies such as 1 uppercase, 1 lowercase etc.

