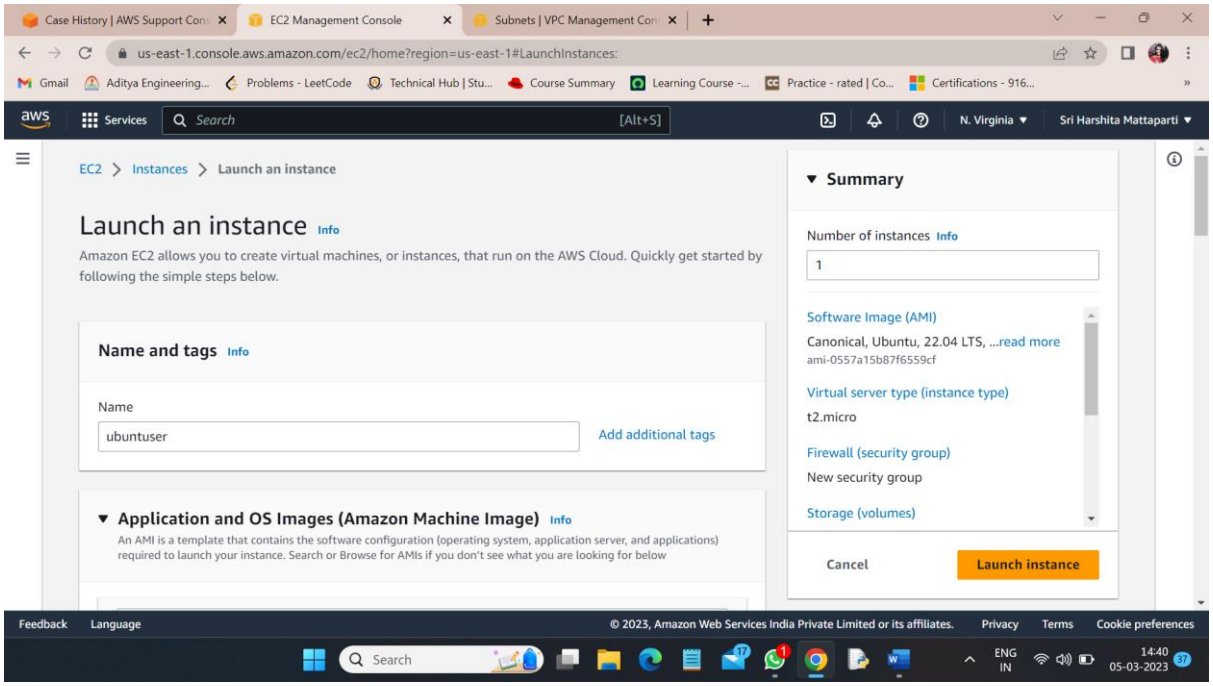
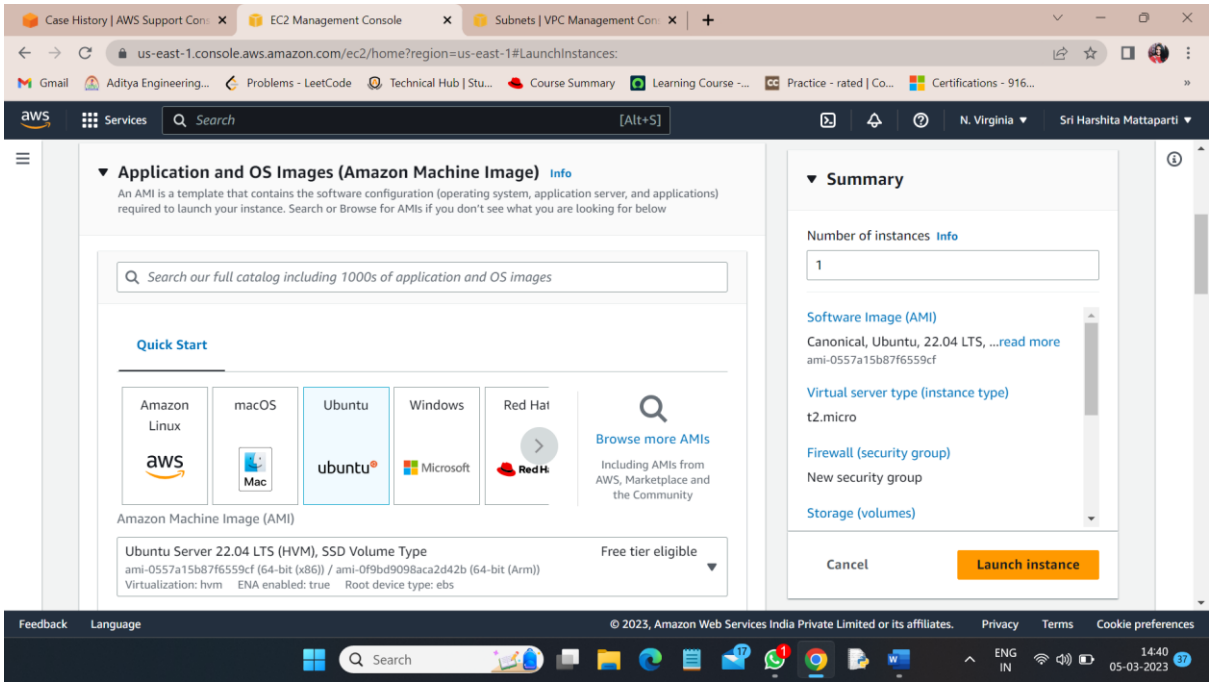
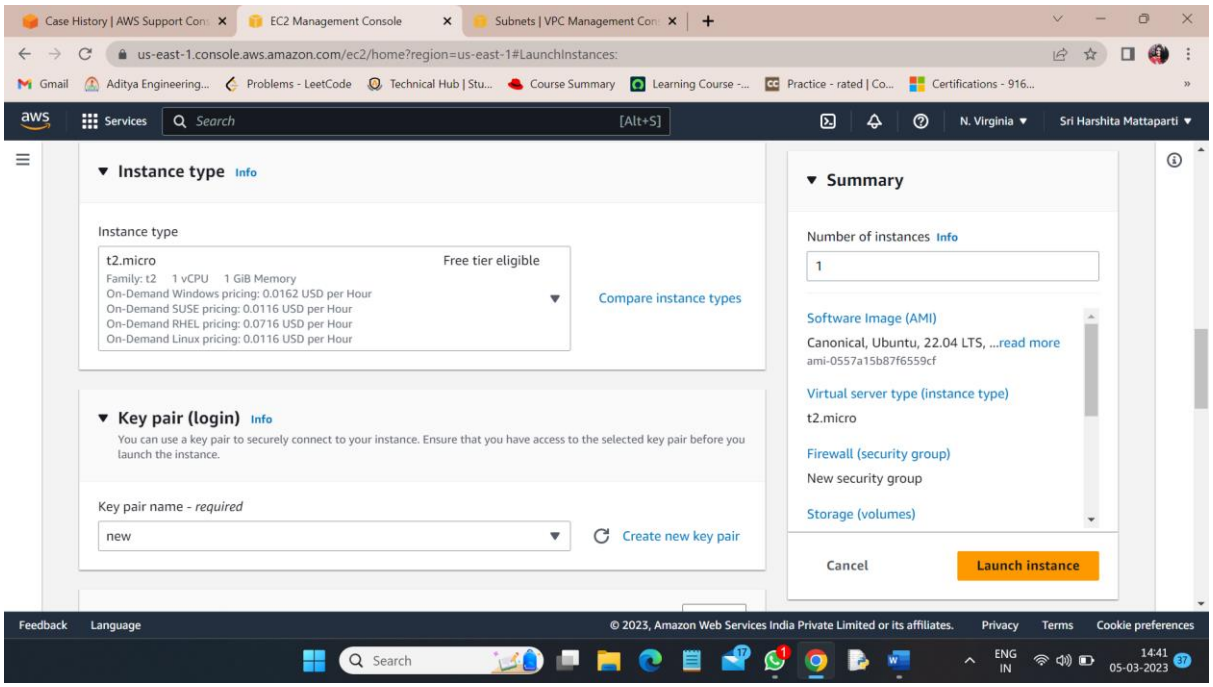
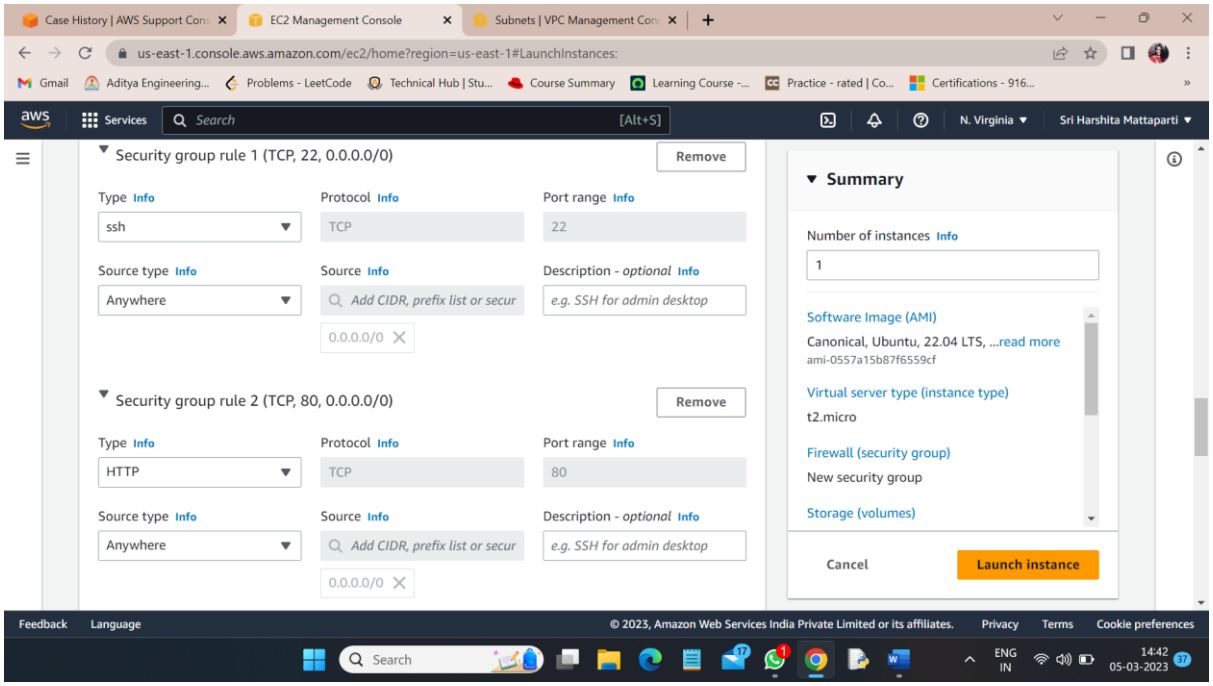
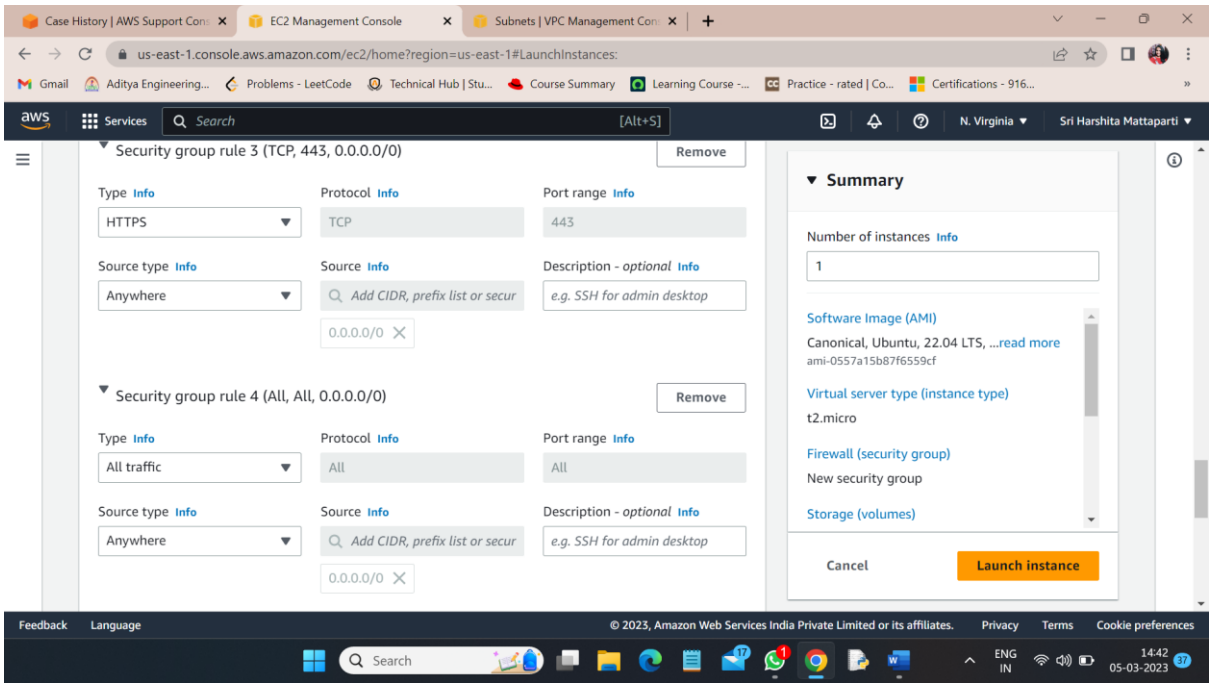
Create an instance with an ubuntu image

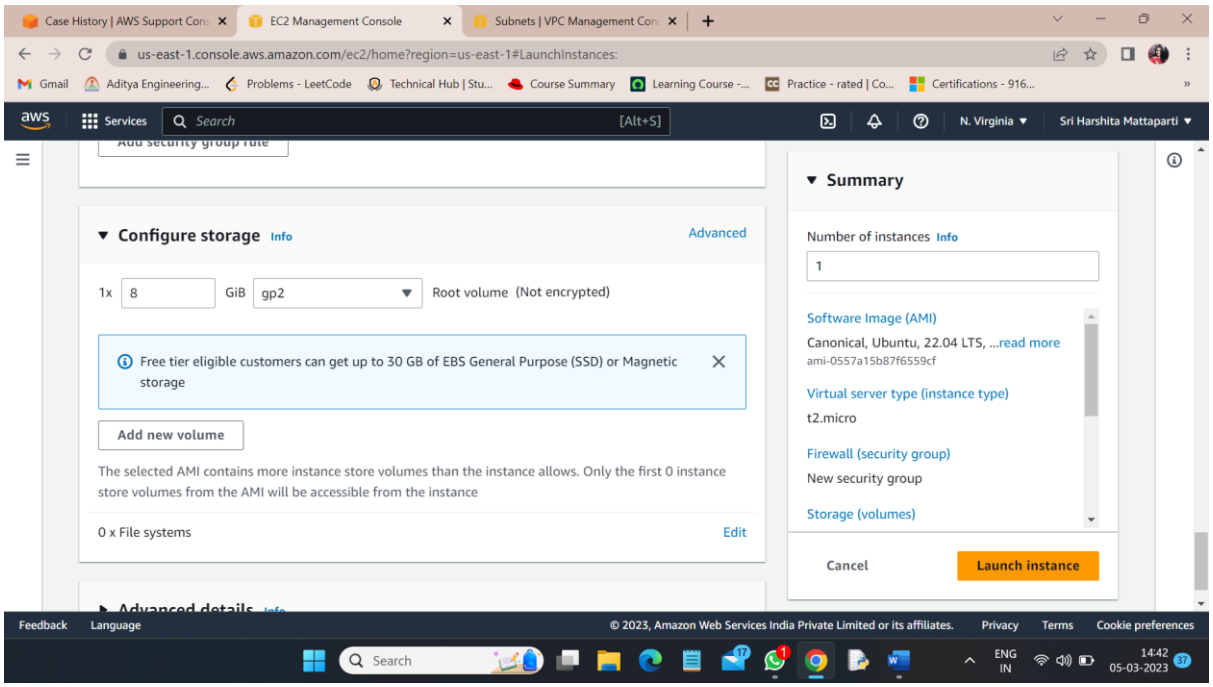


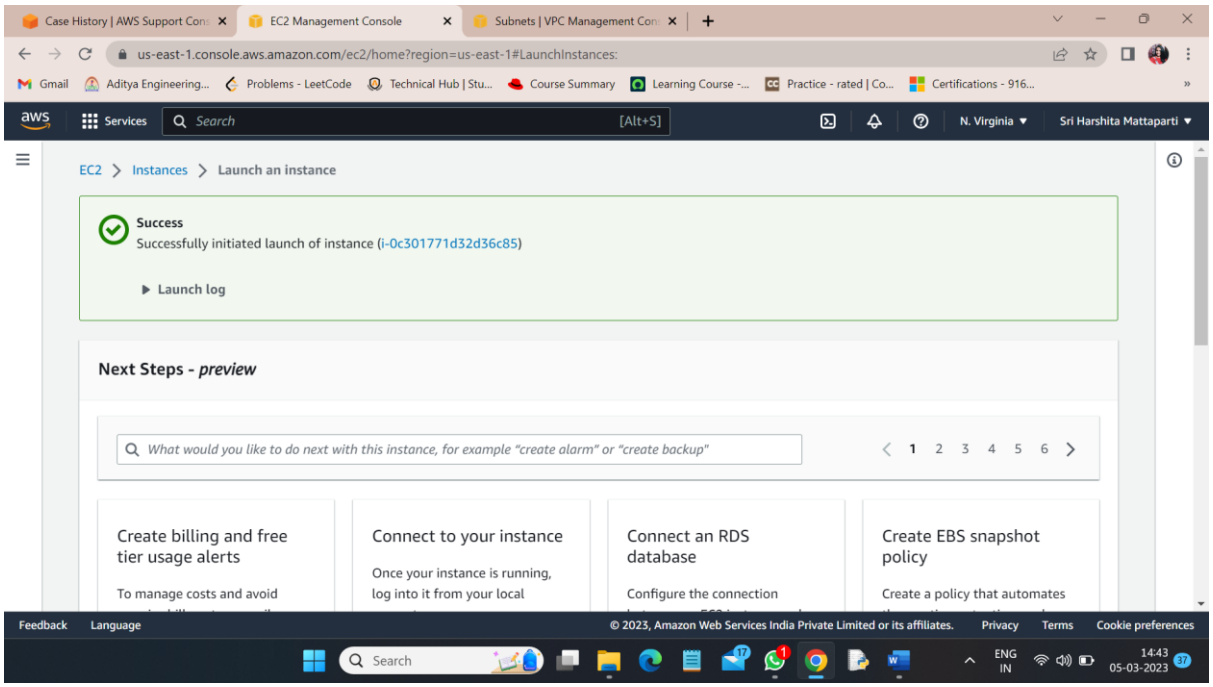



Case History | AWS Support Cons
EC2 Management Console
Subnets | VPC Management Cons
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Gmail
Aditya Engineering...
Problems - LeetCode
Technical Hub | Stu...
Course Summary
Learning Course -...
Practice - rated | Co...
Certifications - 916...
aws
Services
Search
[Alt+S]
N. Virginia
Sri Harshita Mattaparti
Instance type Info
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory
On-Demand Windows pricing: 0.0162 USD per Hour
On-Demand SUSE pricing: 0.0116 USD per Hour
On-Demand RHEL pricing: 0.0716 USD per Hour
On-Demand Linux pricing: 0.0116 USD per Hour
Compare instance types
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
new
Create new key pair
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0557a15b87f6559cf
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
Cancel
Launch instance
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
14:41
05-03-2023

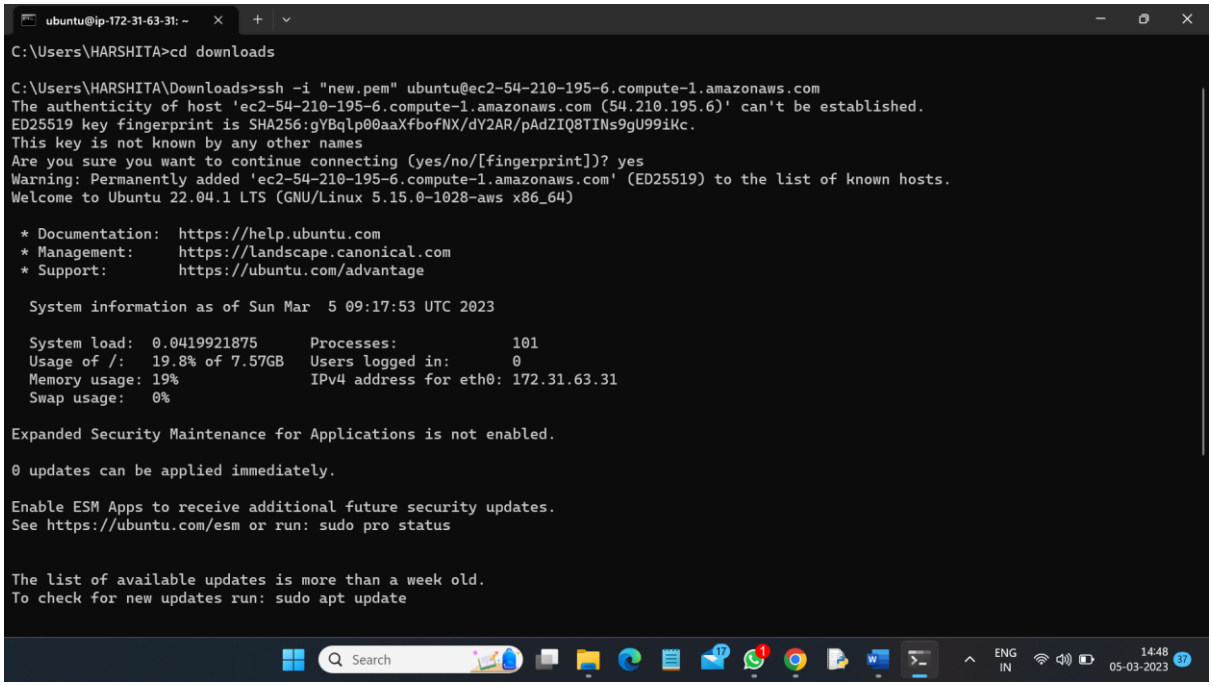

Case History | AWS Support Cons
EC2 Management Console
Subnets | VPC Management Cons
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Gmail
Aditya Engineering...
Problems - LeetCode
Technical Hub | Stu...
Course Summary
Learning Course -...
Practice - rated | Co...
Certifications - 916...
aws
Services
Search
[Alt+S]
N. Virginia
Sri Harshita Mattaparti
Security group rule 1 (TCP, 22, 0.0.0.0/0)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or secur
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Security group rule 2 (TCP, 80, 0.0.0.0/0)
Remove
Type Info
HTTP
Protocol Info
TCP
Port range Info
80
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or secur
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0557a15b87f6559cf
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
Cancel
Launch instance
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
14:42
05-03-2023


Case History | AWS Support Cons
EC2 Management Console
Subnets | VPC Management Cons
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Gmail
Aditya Engineering...
Problems - LeetCode
Technical Hub | Stu...
Course Summary
Learning Course -...
Practice - rated | Co...
Certifications - 916...
aws
Services
Search
[Alt+S]
N. Virginia
Sri Harshita Mattaparti
Security group rule 3 (TCP, 443, 0.0.0.0/0)
Remove
Type Info
HTTPS
Protocol Info
TCP
Port range Info
443
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or secur
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Security group rule 4 (All, All, 0.0.0.0/0)
Remove
Type Info
All traffic
Protocol Info
All
Port range Info
All
Source type Info
Anywhere
Source Info
Add CIDR, prefix list or secur
0.0.0.0/0
Description - optional Info
e.g. SSH for admin desktop
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0557a15b87f6559cf
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
Cancel
Launch instance
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
14:42
05-03-2023

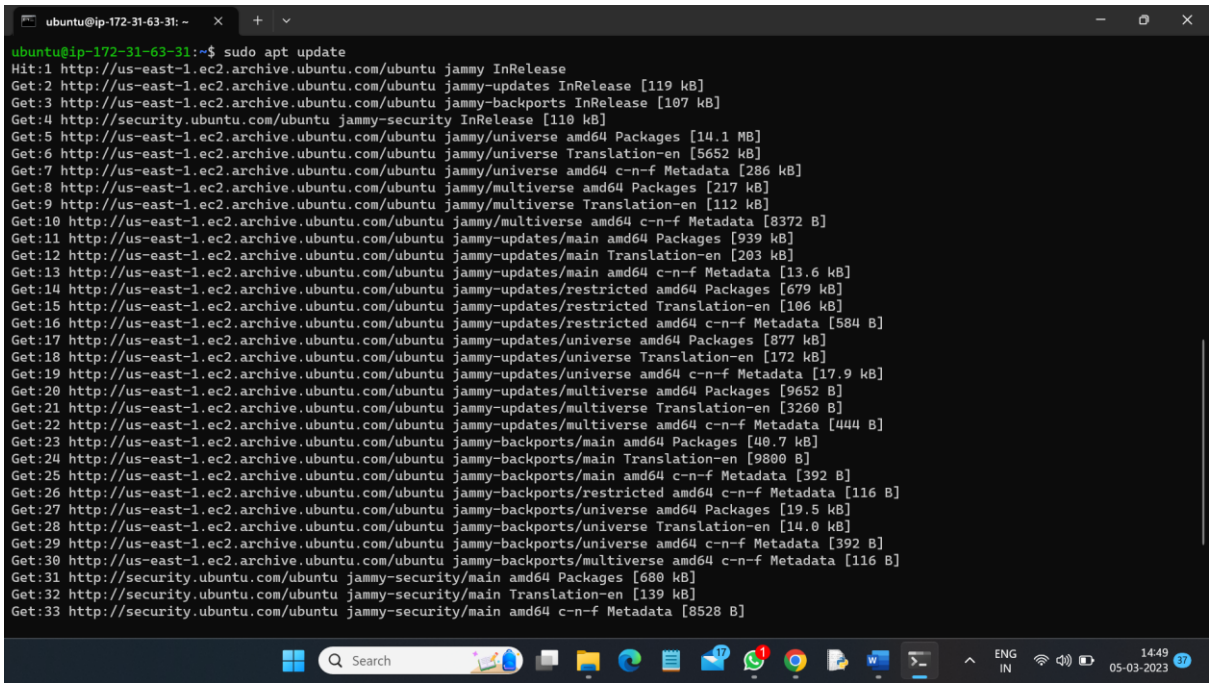

Case History | AWS Support Cons
EC2 Management Console
Subnets | VPC Management Cons
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:
Gmail
Aditya Engineering...
Problems - LeetCode
Technical Hub | Stu...
Course Summary
Learning Course -...
Practice - rated | Co...
Certifications - 916...
aws
Services
Search
[Alt+S]
N. Virginia
Sri Harshita Mattaparti
Configure storage Info
Advanced
1x
8
GiB
gp2
Root volume (Not encrypted)
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage
Add new volume
The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance
0 x File systems
Edit
Summary
Number of instances Info
1
Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0557a15b87f6559cf
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
Cancel
Launch instance
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
14:42
05-03-2023



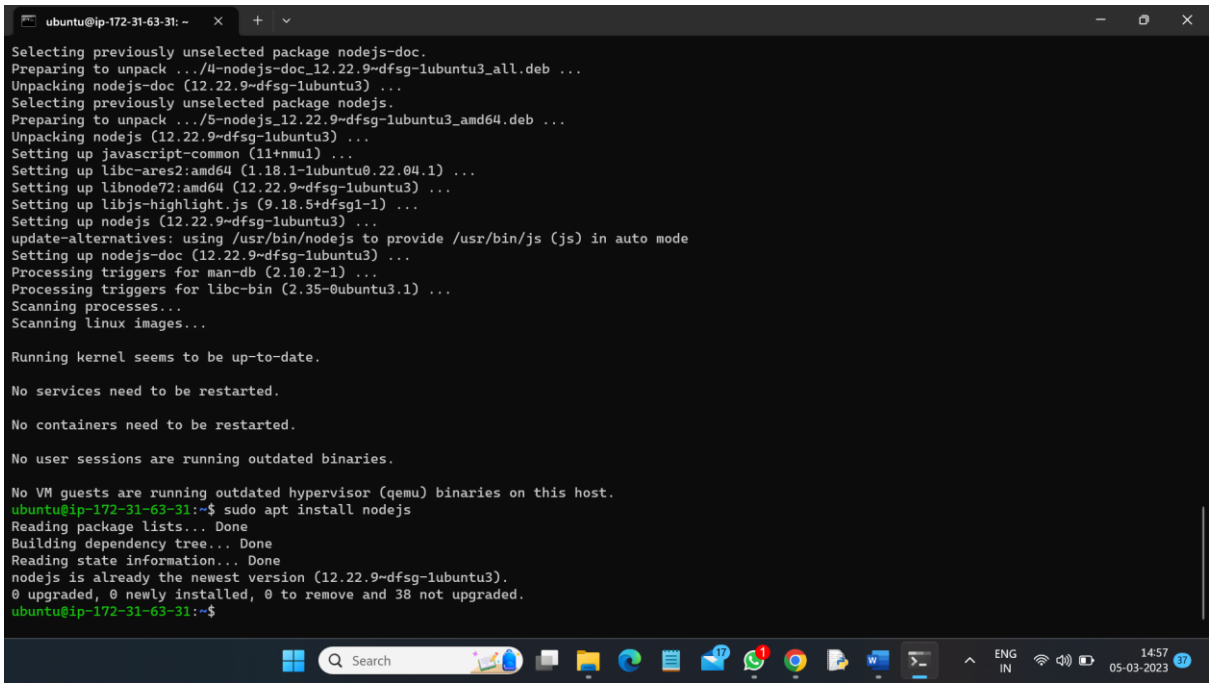
Copy and paste the ssh command



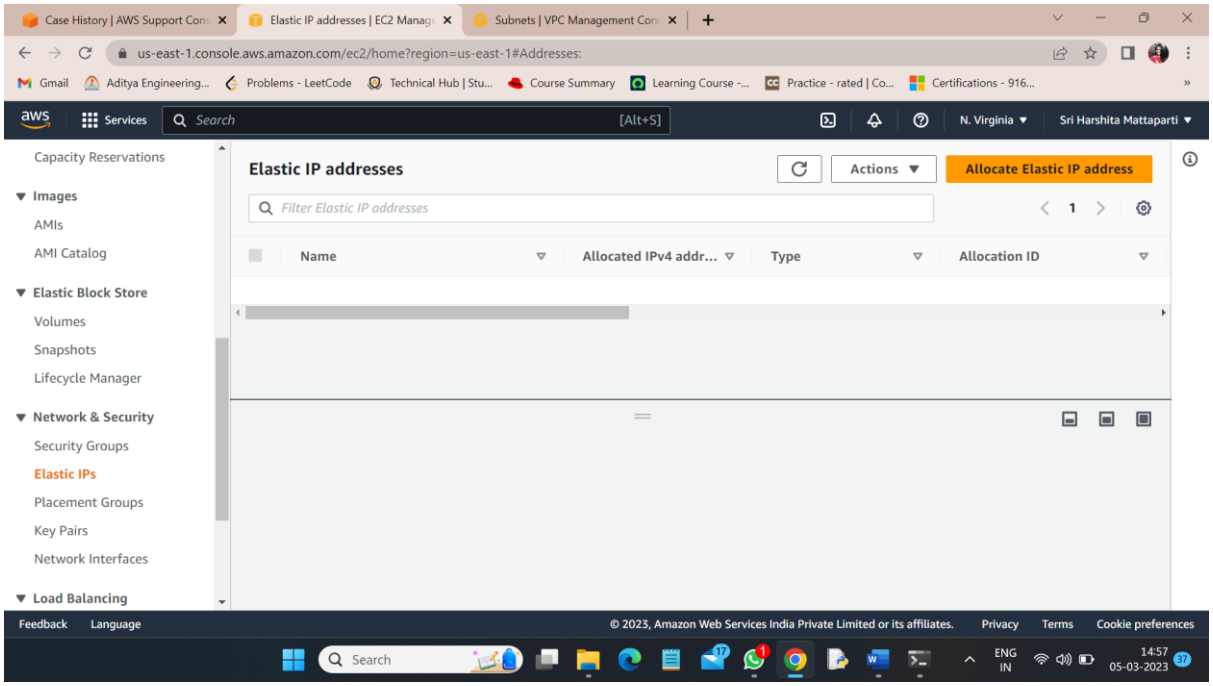
Give sudo apt update

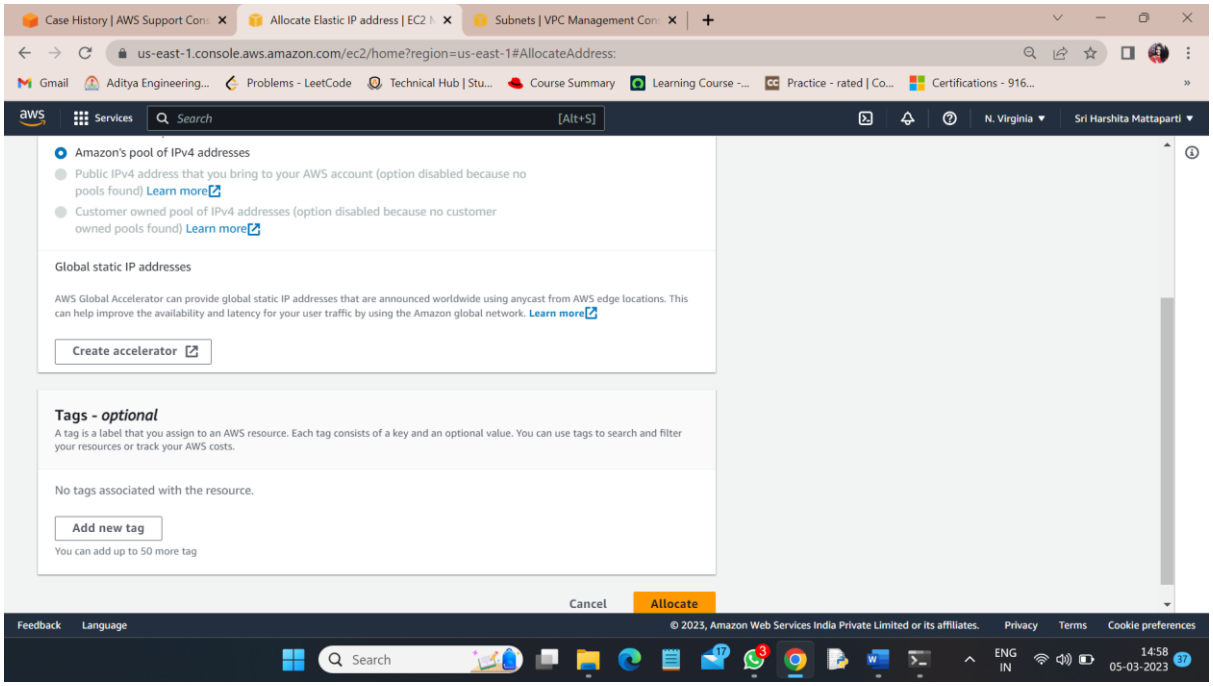


Install nodejs by giving sudo install nodejs

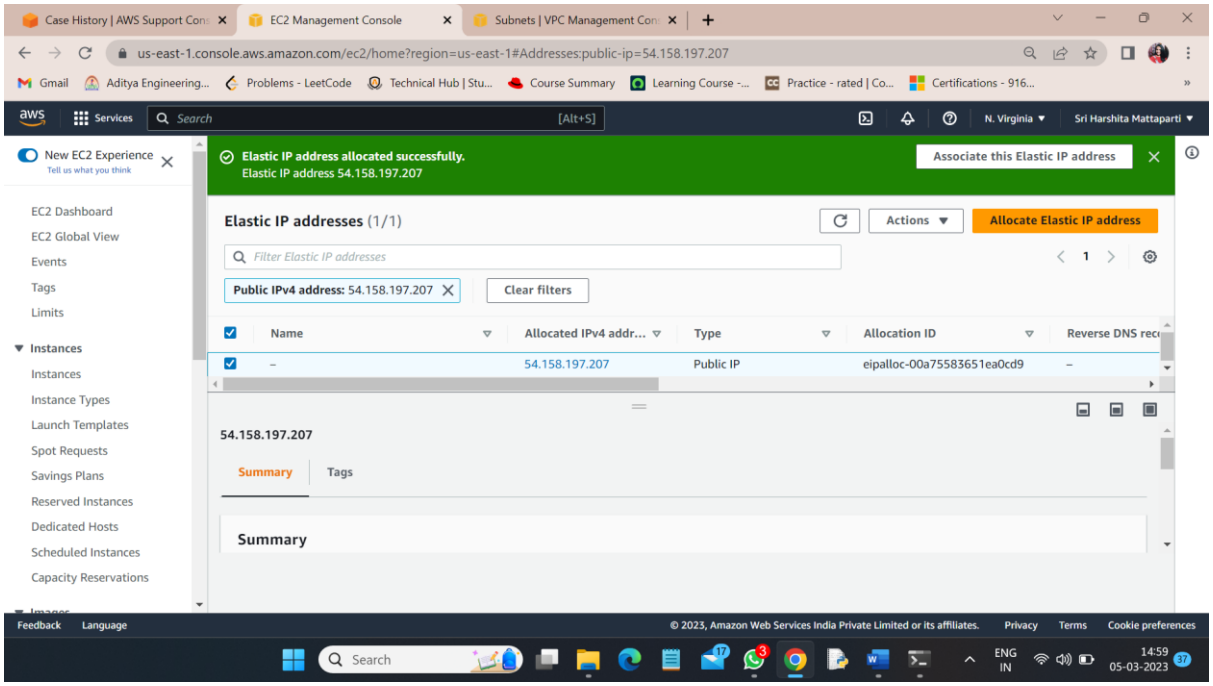


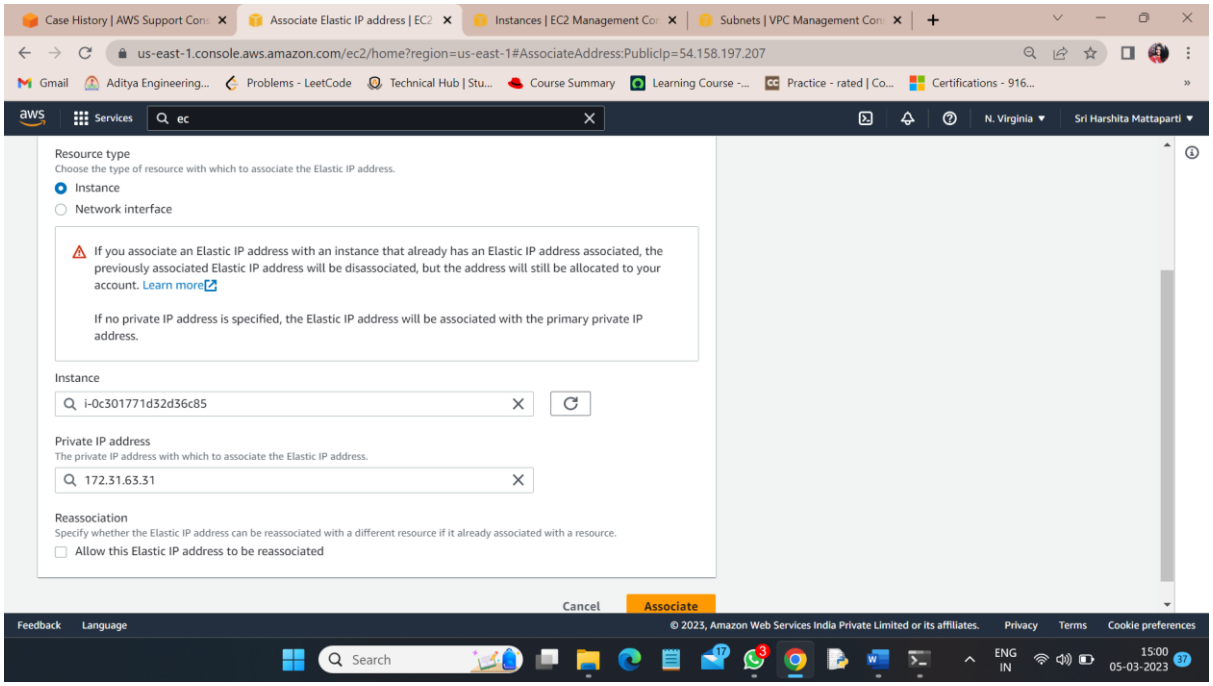
Now allocate an Elastic IP address



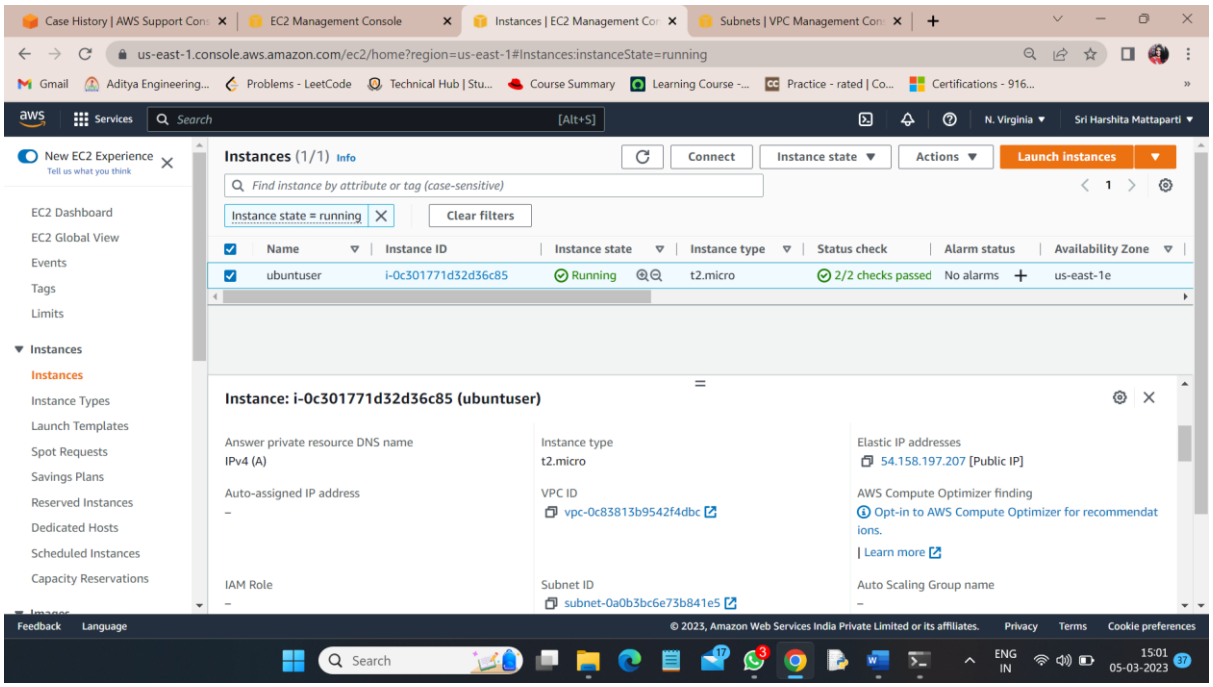


Associate the Elastic IP with the Instance

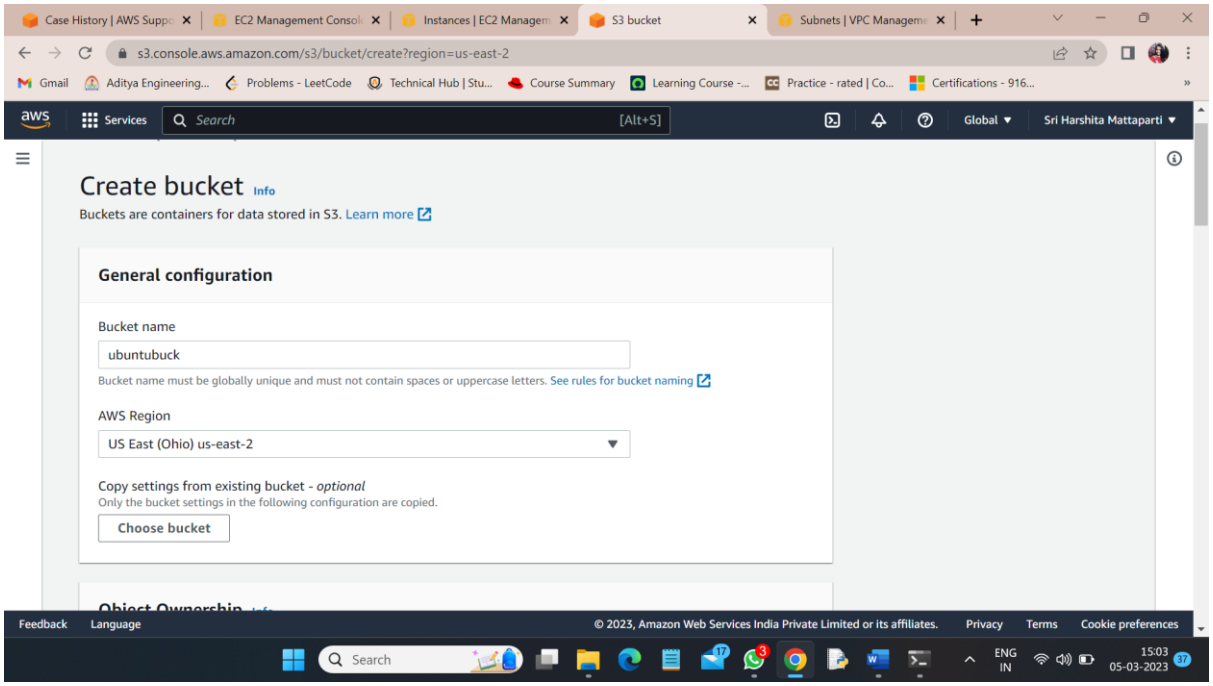


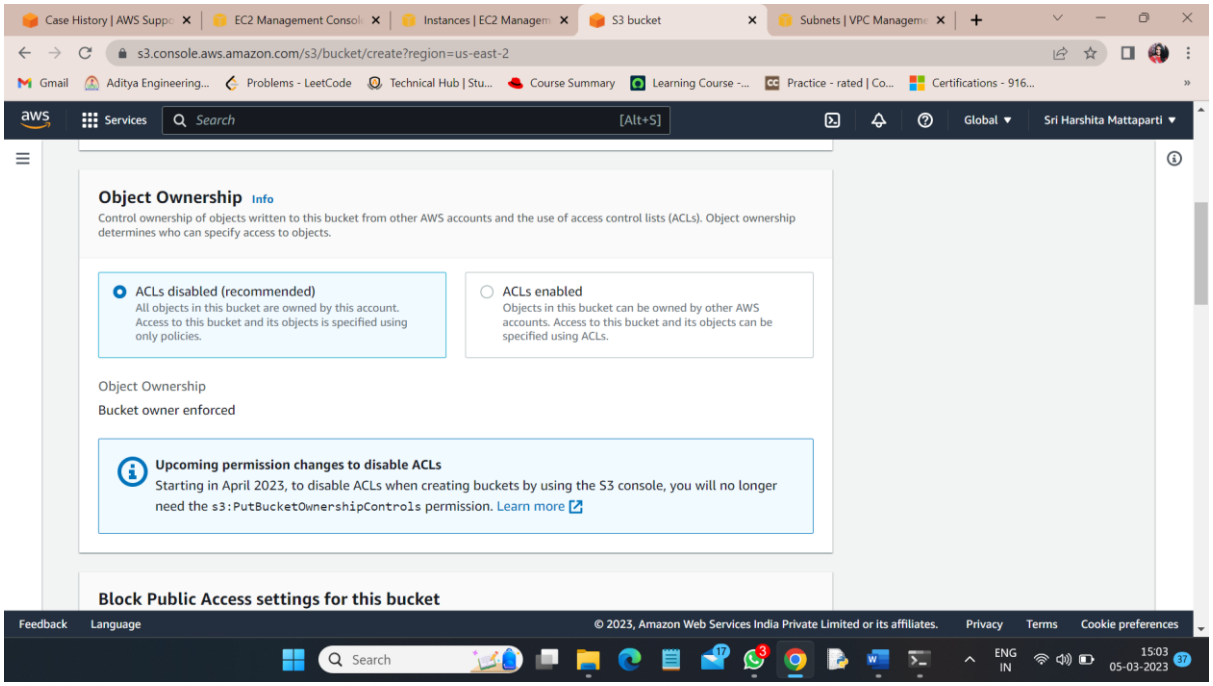


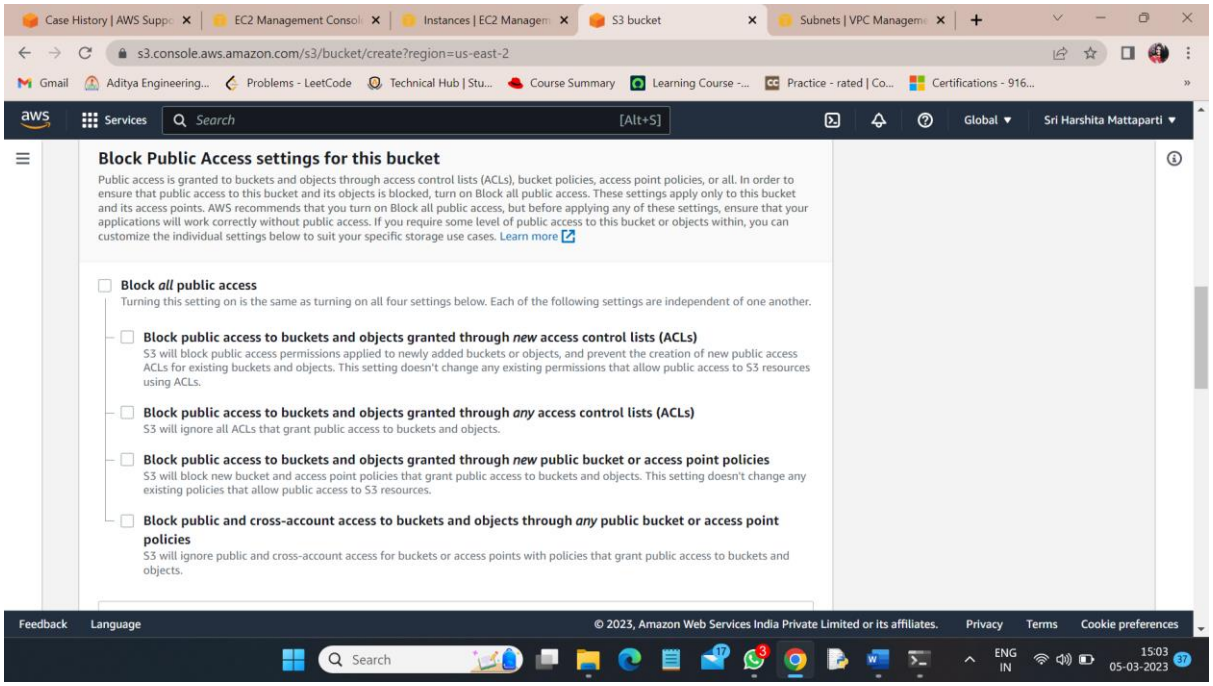
Instance has been associated

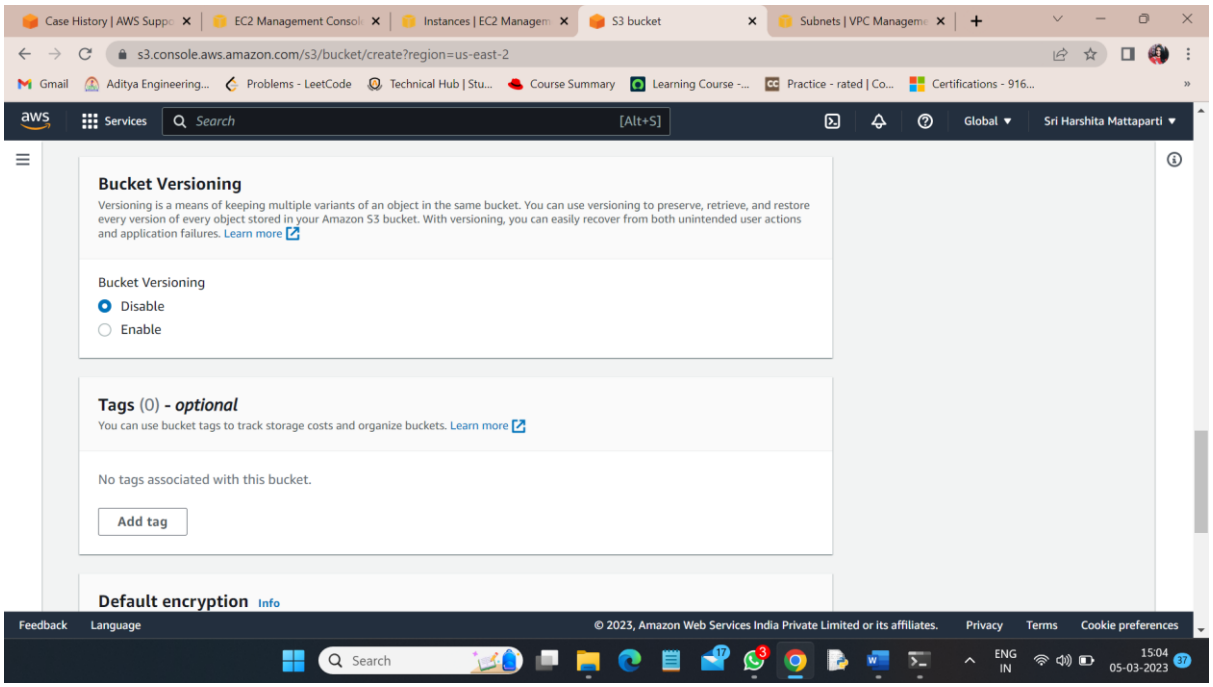


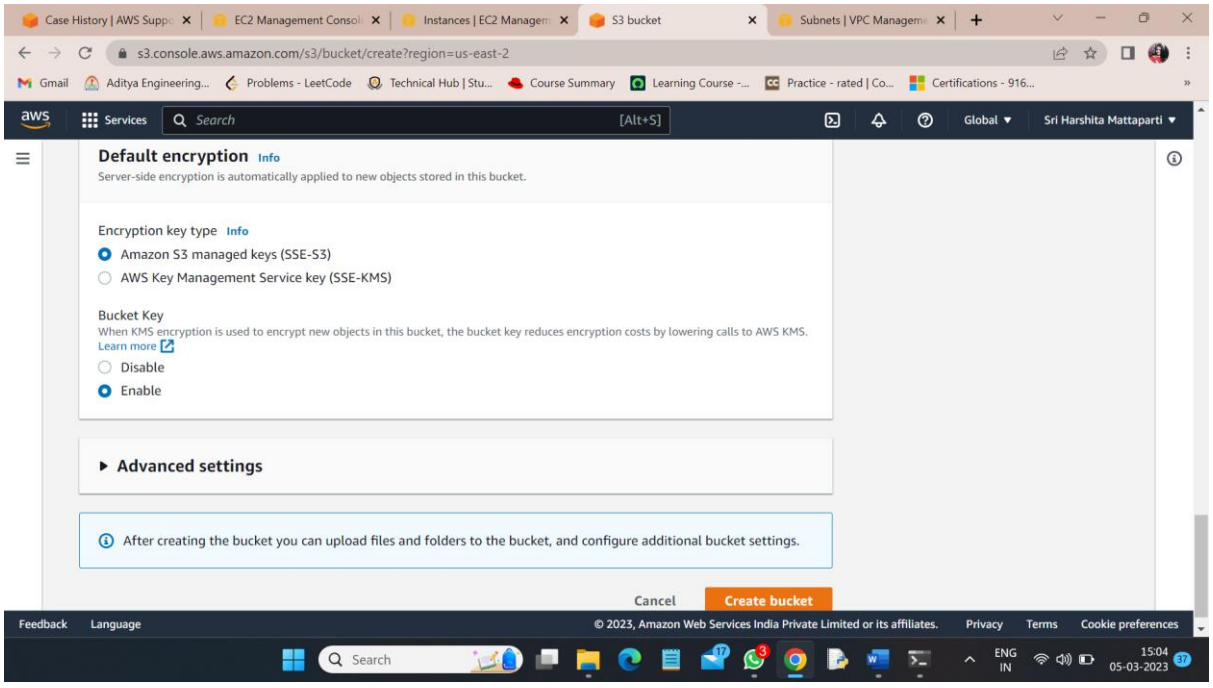
Now create an S3 bucket

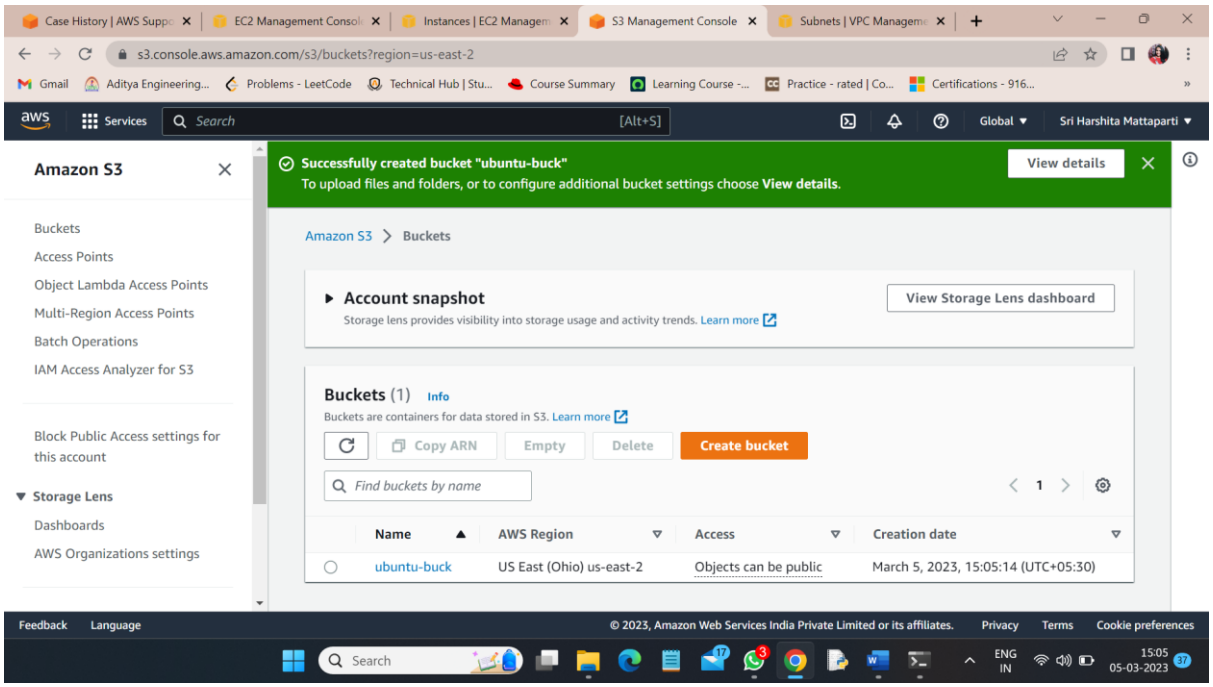



Case History | AWS Suppo
EC2 Management Consol
Instances | EC2 Managem
S3 bucket
Subnets | VPC Manageme
s3.console.aws.amazon.com/s3/bucket/create?region=us-east-2
Gmail
Aditya Engineering...
Problems - LeetCode
Technical Hub | Stu...
Course Summary
Learning Course -...
Practice - rated | Co...
Certifications - 916...
aws
Services
Search
[Alt+S]
Global
Sri Harshita Mattaparti
Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
Object Ownership
Bucket owner enforced
Upcoming permission changes to disable ACLs
Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you will no longer need the s3:PutBucketOwnershipControls permission. Learn more
Block Public Access settings for this bucket
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
15:03
05-03-2023

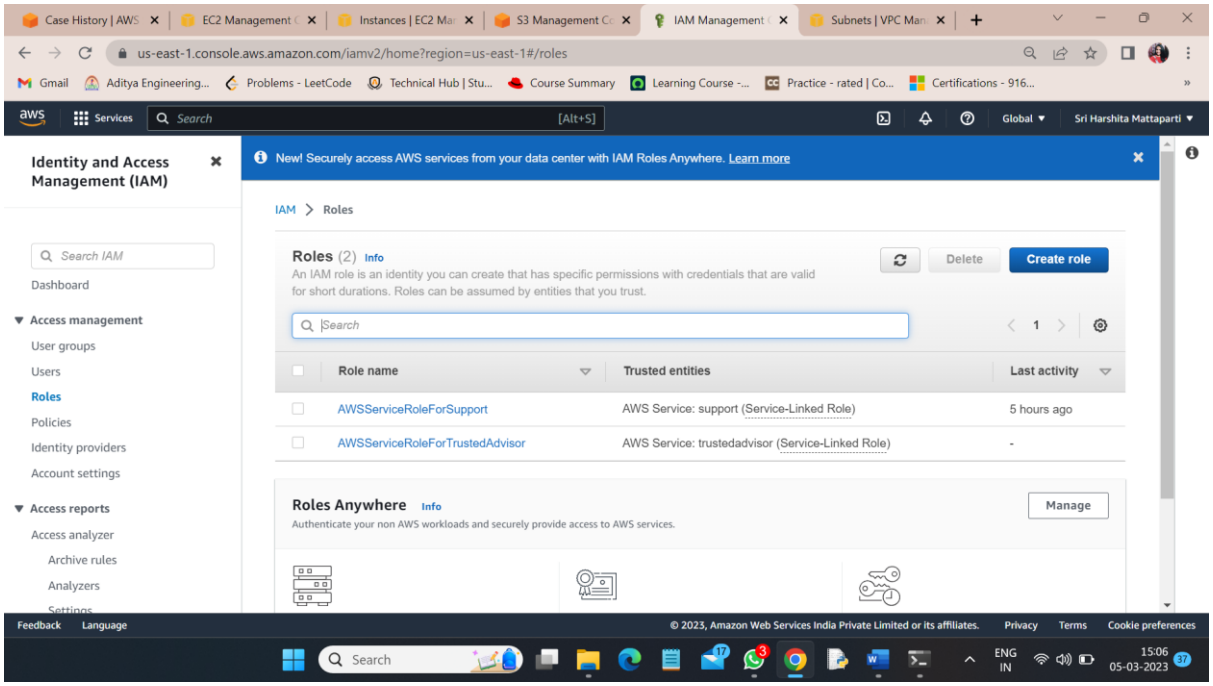

Case History | AWS Suppo
EC2 Management Consol
Instances | EC2 Managem
S3 bucket
Subnets | VPC Manageme
s3.console.aws.amazon.com/s3/bucket/create?region=us-east-2
Gmail
Aditya Engineering...
Problems - LeetCode
Technical Hub | Stu...
Course Summary
Learning Course -...
Practice - rated | Co...
Certifications - 916...
aws
Services
Search
[Alt+S]
Global
Sri Harshita Mattaparti
Block Public Access settings for this bucket
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 this bucket and its 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 this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
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.
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
15:03
05-03-2023


Case History | AWS Supp
EC2 Management Consol
Instances | EC2 Managem
S3 bucket
Subnets | VPC Managem
s3.console.aws.amazon.com/s3/bucket/create?region=us-east-2
Gmail
Aditya Engineering...
Problems - LeetCode
Technical Hub | Stu...
Course Summary
Learning Course -...
Practice - rated | Co...
Certifications - 916...
aws
Services
Search
[Alt+S]
Global
Sri Harshita Mattaparti
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 (0) - optional
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
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
15:04
05-03-2023

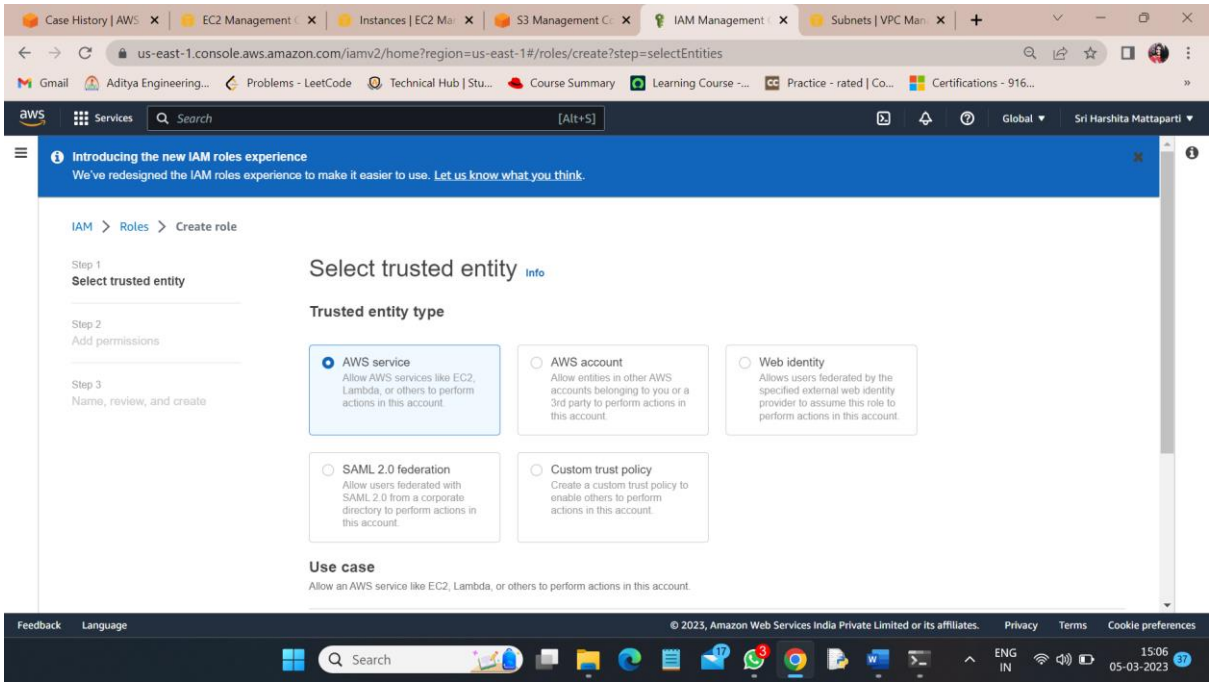

Case History | AWS Supp
EC2 Management Consol
Instances | EC2 Managem
S3 bucket
Subnets | VPC Managem
s3.console.aws.amazon.com/s3/bucket/create?region=us-east-2
Gmail
Aditya Engineering...
Problems - LeetCode
Technical Hub | Stu...
Course Summary
Learning Course -...
Practice - rated | Co...
Certifications - 916...
aws
Services
Search
[Alt+S]
Global
Sri Harshita Mattaparti
Default encryption Info
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption key type Info
Amazon S3 managed keys (SSE-S3)
AWS Key Management Service key (SSE-KMS)
Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS.
Learn more
Disable
Enable
Advanced settings
After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.
Cancel
Create bucket
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
Search
ENG
IN
15:04
05-03-2023

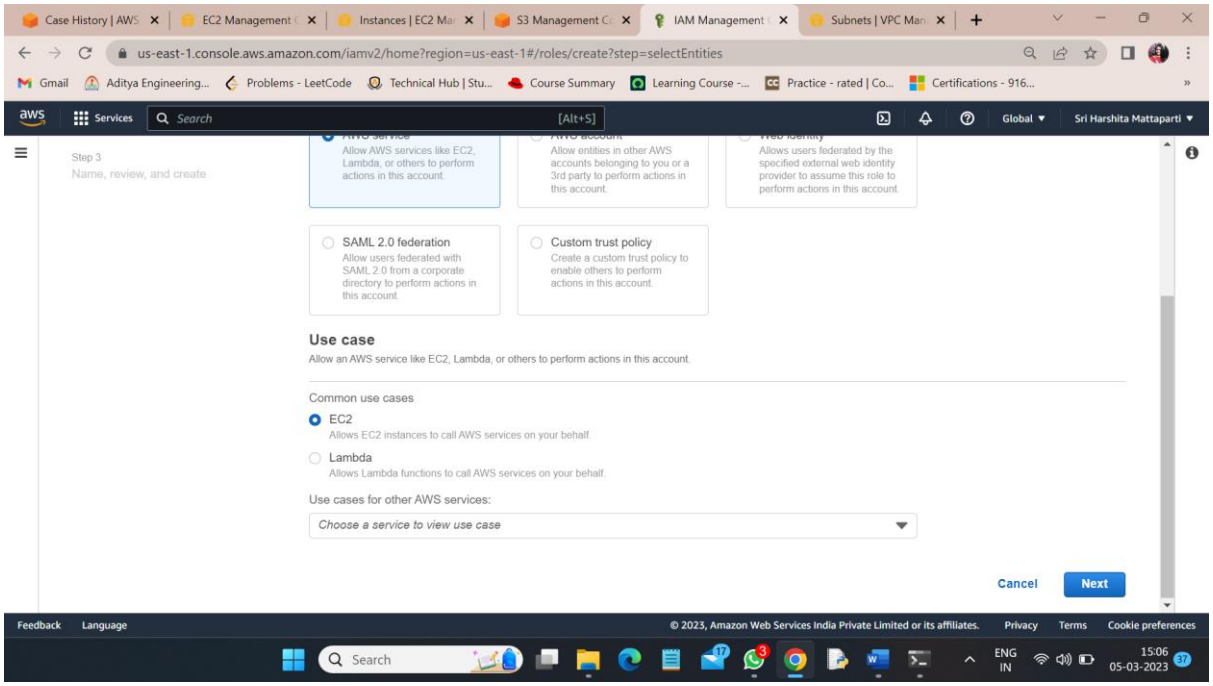


Create an IAM Role for uploading objects

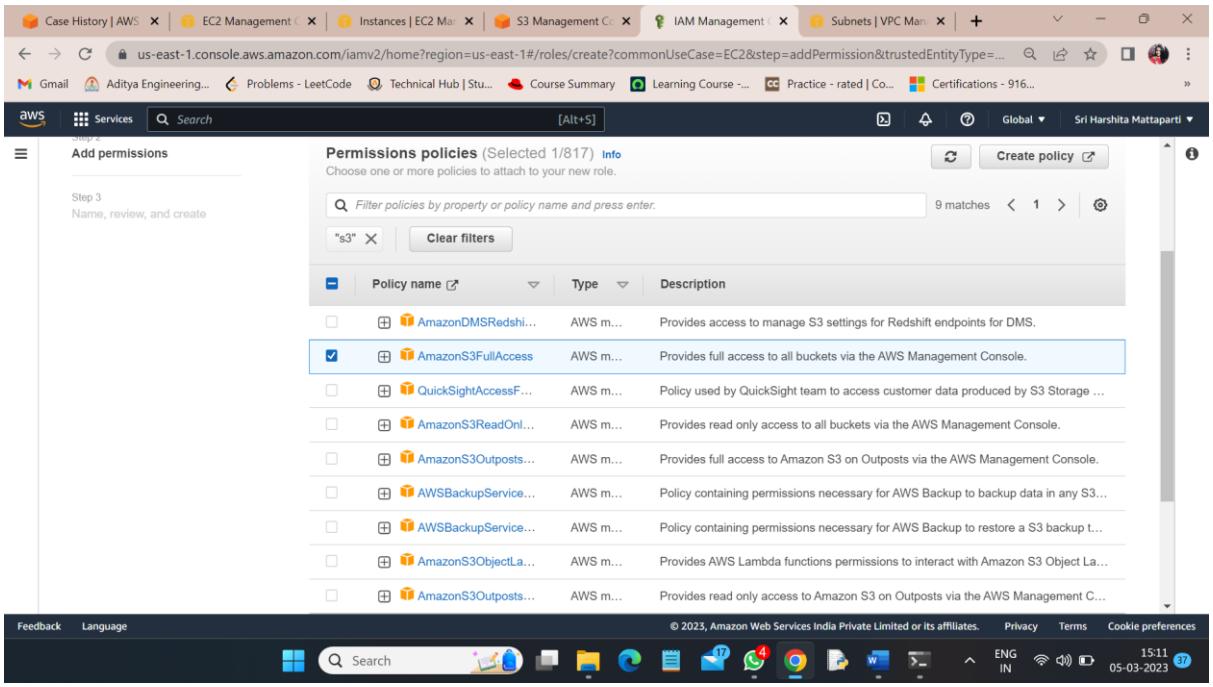


Select an Entity

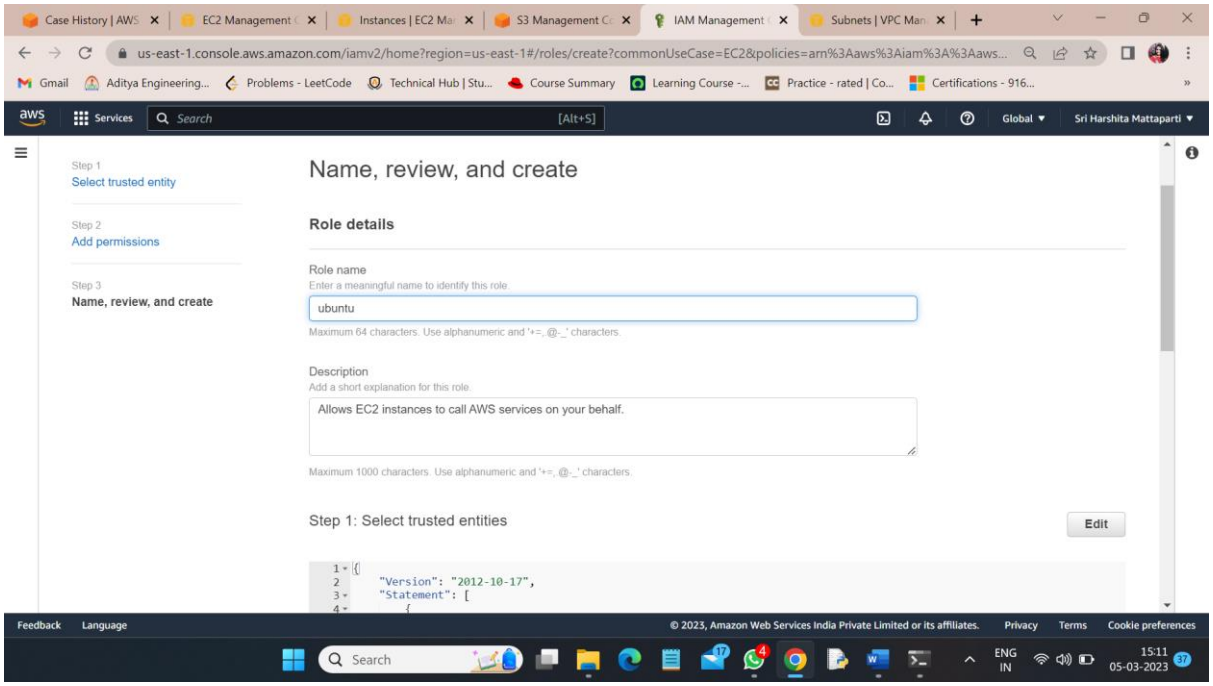


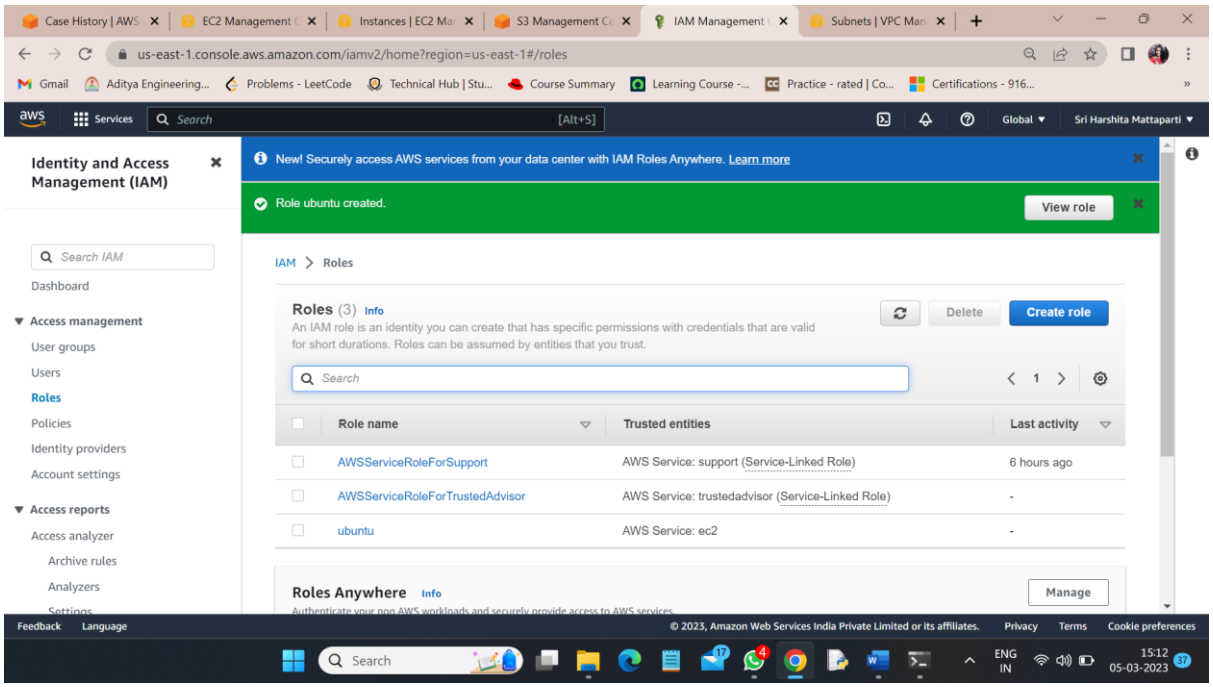


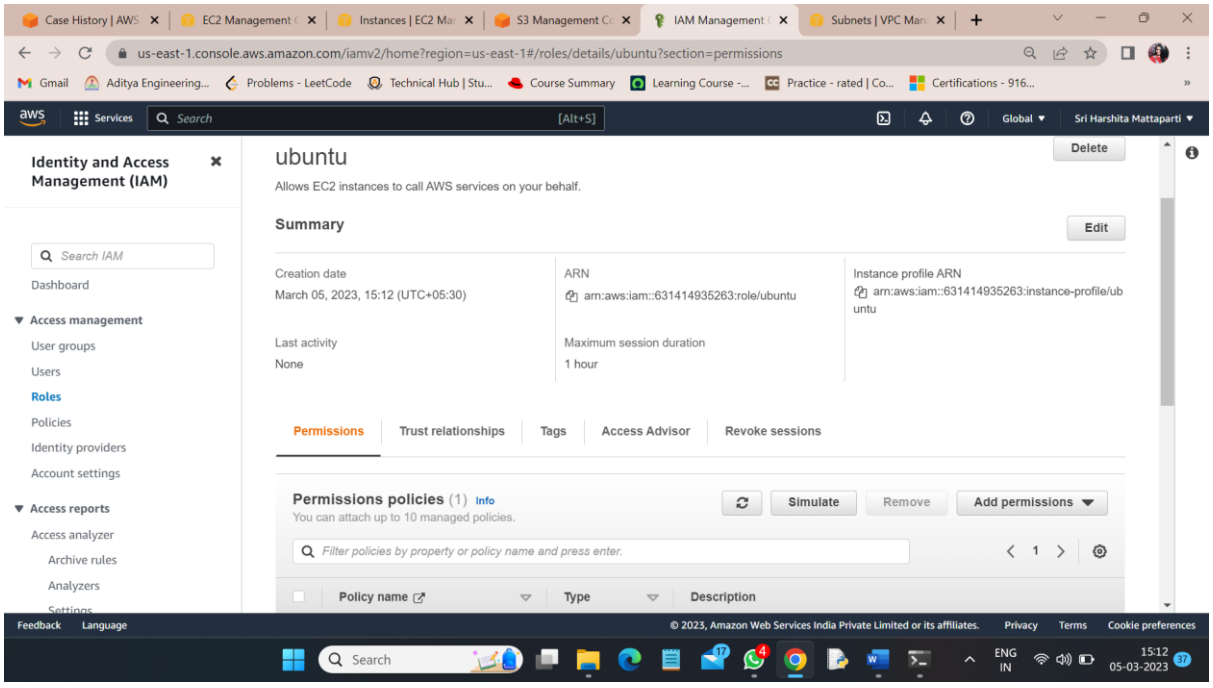
Select the Policy



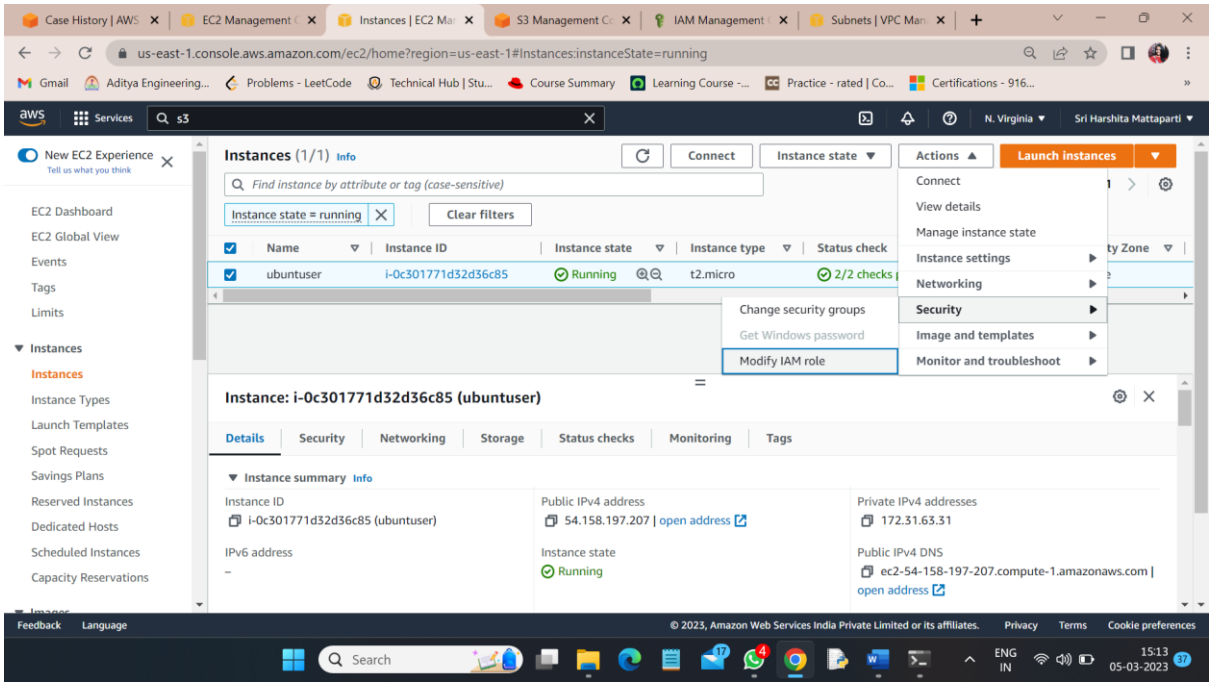
Give a name to the role

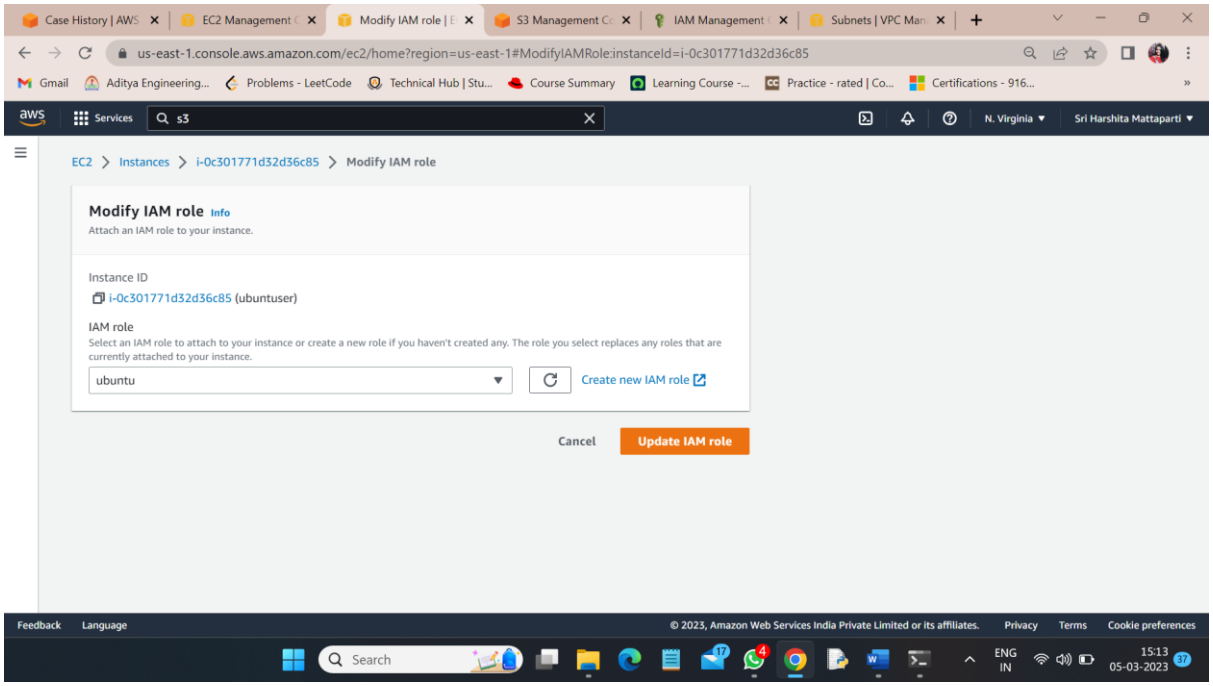


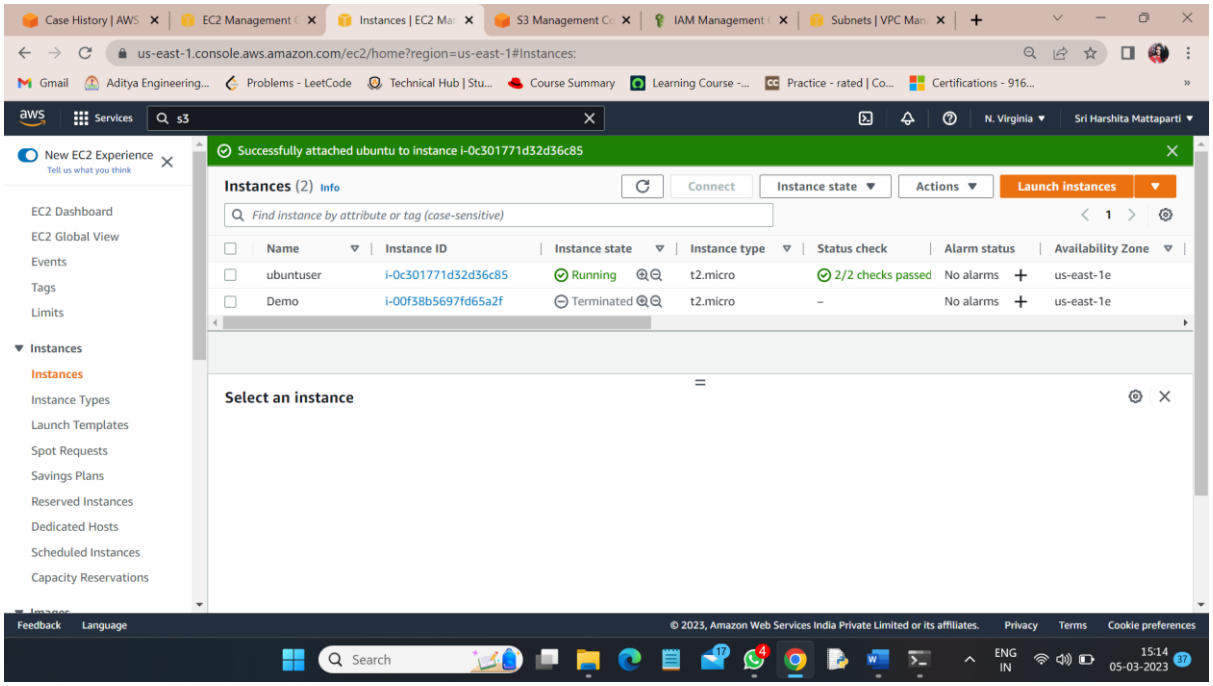

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles
Identity and Access Management (IAM)
New! Securely access AWS services from your data center with IAM Roles Anywhere. Learn more
Role ubuntu created.
View role
IAM > Roles
Roles (3) Info
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.
Delete
Create role
Role name
Trusted entities
Last activity
AWSServiceRoleForSupport
AWS Service: support (Service-Linked Role)
6 hours ago
AWSServiceRoleForTrustedAdvisor
AWS Service: trustedadvisor (Service-Linked Role)
ubuntu
AWS Service: ec2
Roles Anywhere Info
Manage


us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/details/ubuntu?section=permissions
Identity and Access Management (IAM)
ubuntu
Allows EC2 instances to call AWS services on your behalf.
Delete
Summary
Edit
Creation date
March 05, 2023, 15:12 (UTC+05:30)
ARN
arn:aws:iam::631414935263:role/ubuntu
Instance profile ARN
arn:aws:iam::631414935263:instance-profile/ubuntu
Last activity
None
Maximum session duration
1 hour
Permissions
Trust relationships
Tags
Access Advisor
Revoke sessions
Permissions policies (1) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter policies by property or policy name and press enter.
Policy name
Type
Description

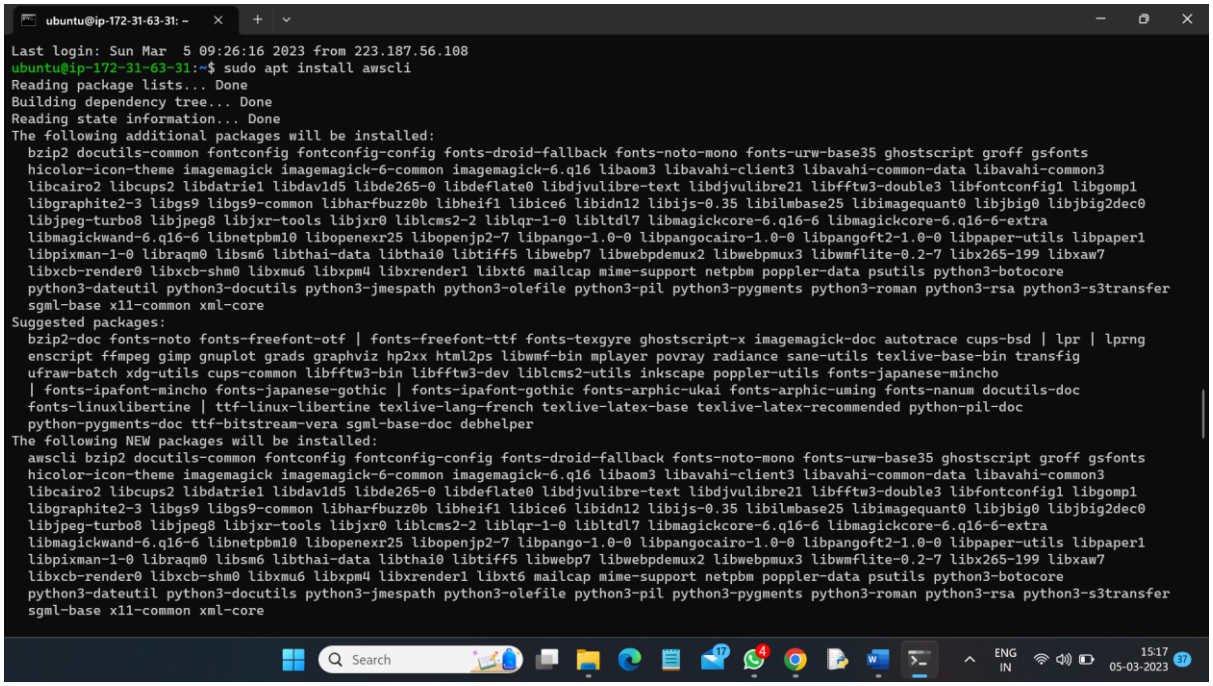
Assign Instance with the Role



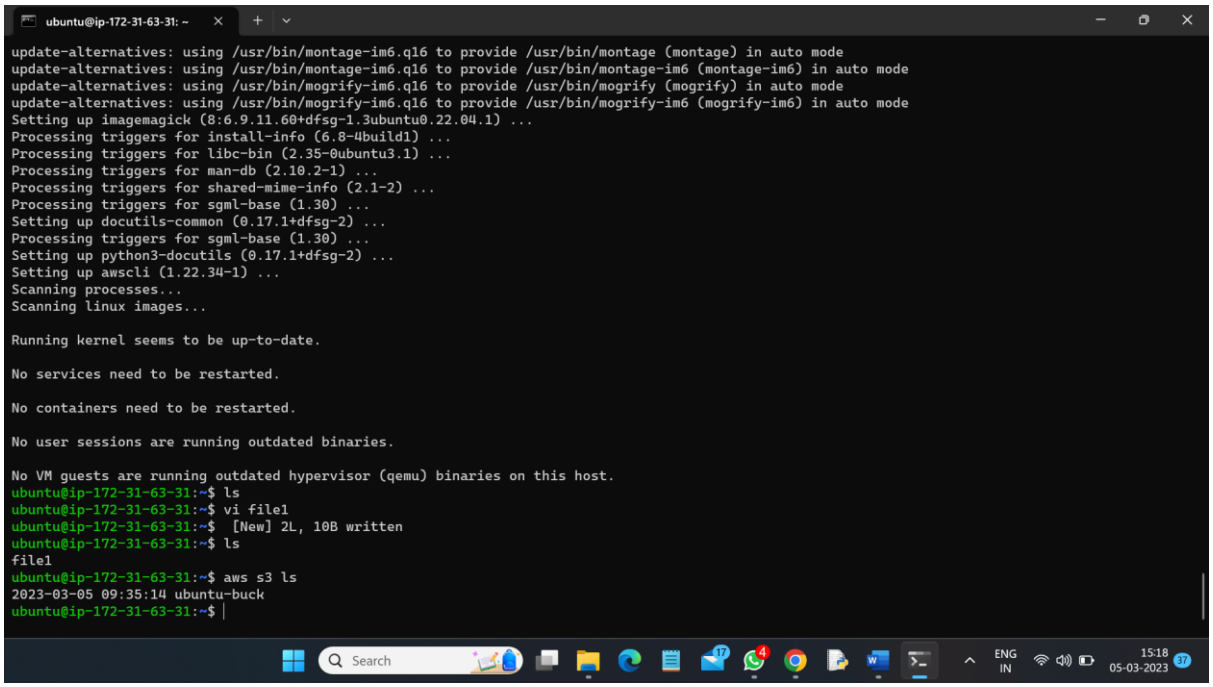




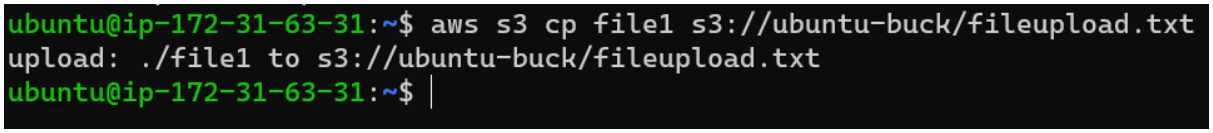
Now give sudo apt install awscli



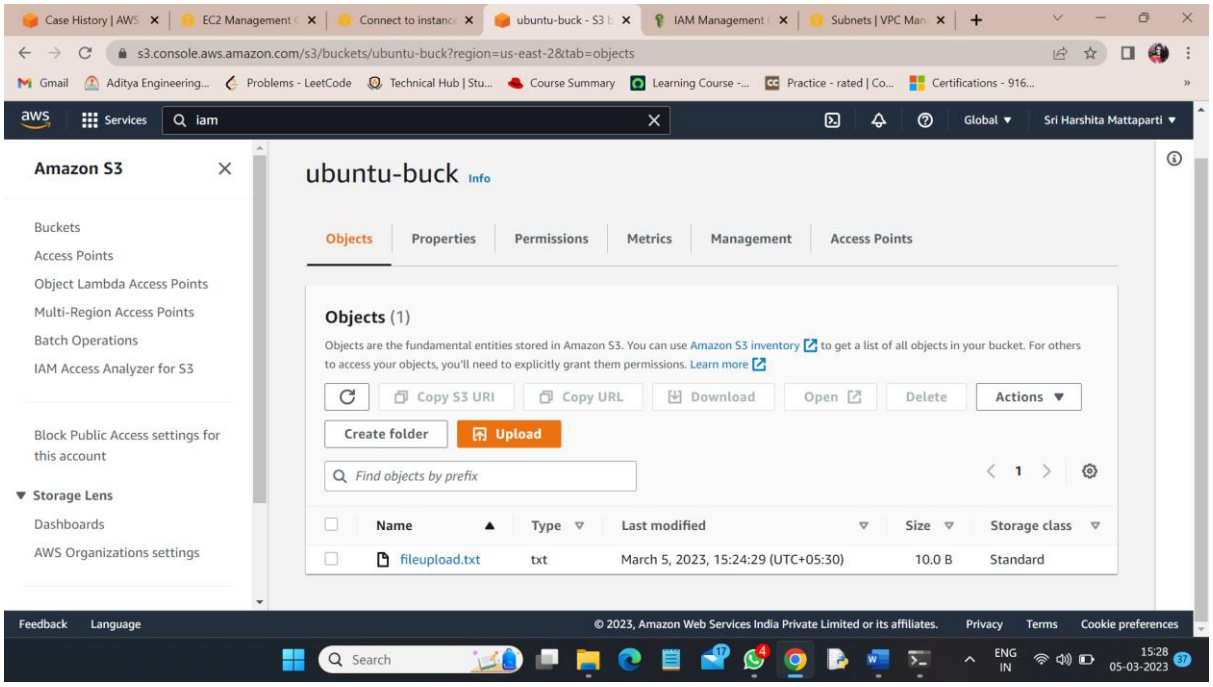
Now create any file, aws s3 ls command will give the list of buckets in S3



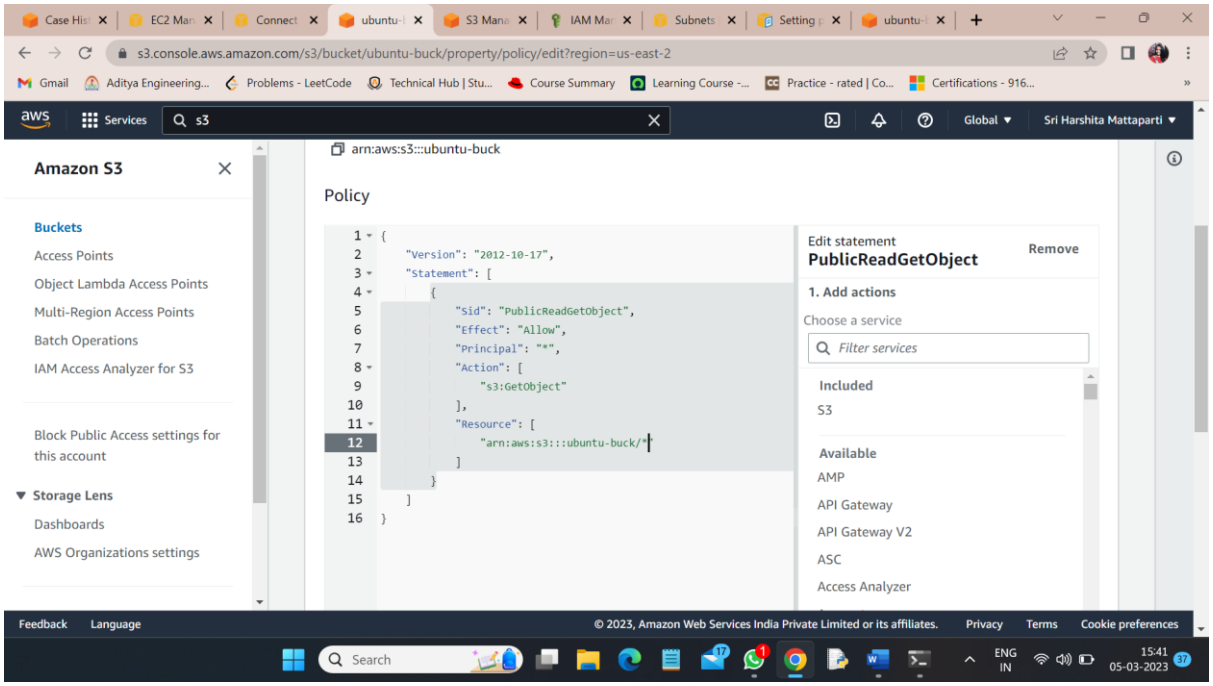
Upload the file into the bucket



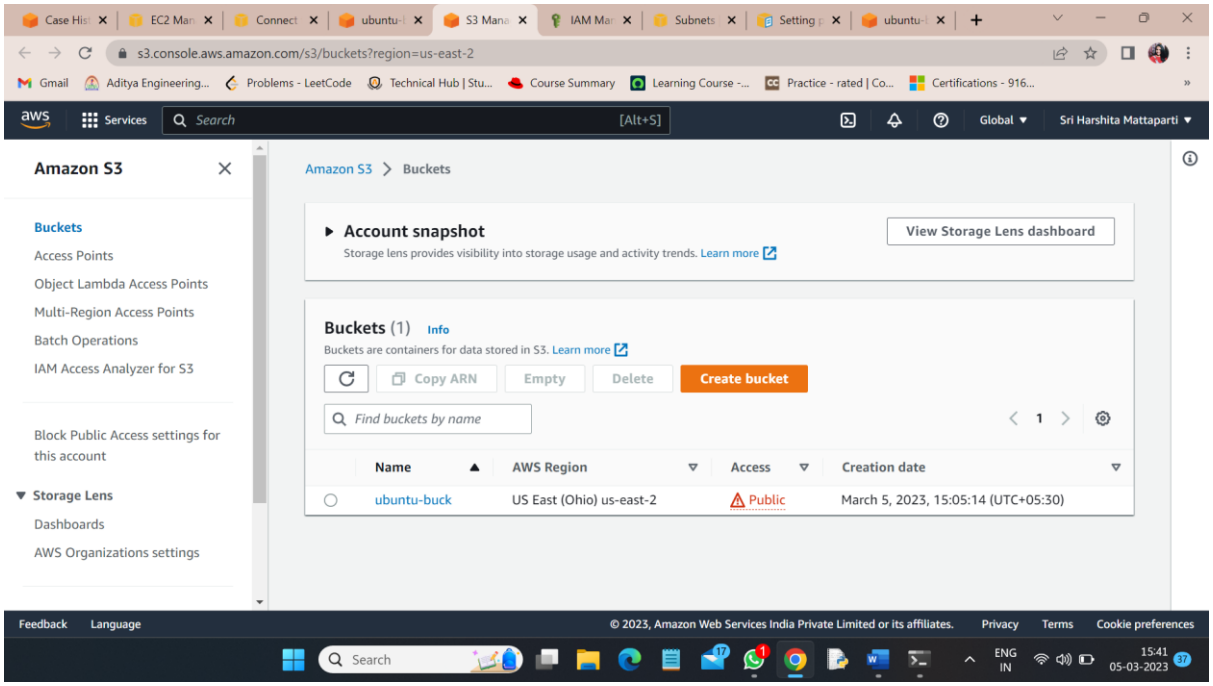
The file has been uploaded



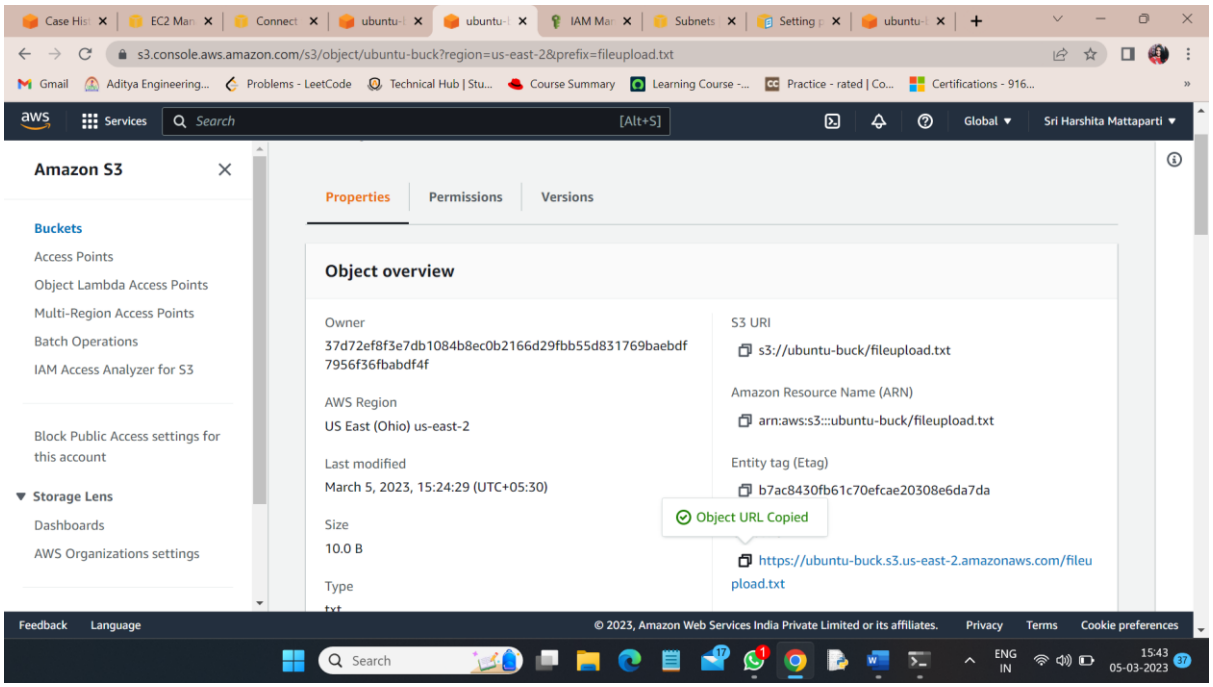
Now edit the bucket policy



Now the object has got the public access



Copy the object url



Paste the url in the browser