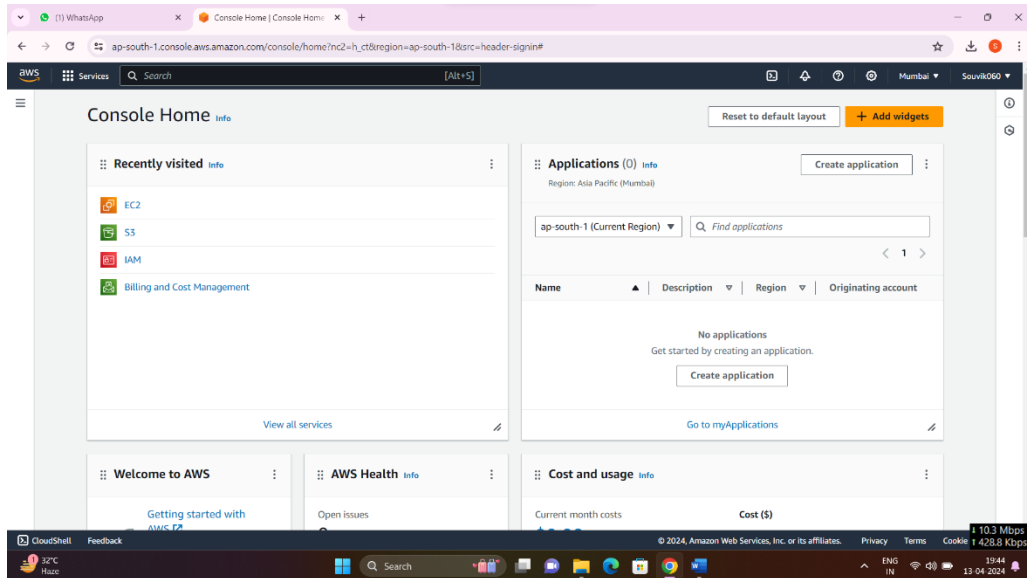


Assignment 10

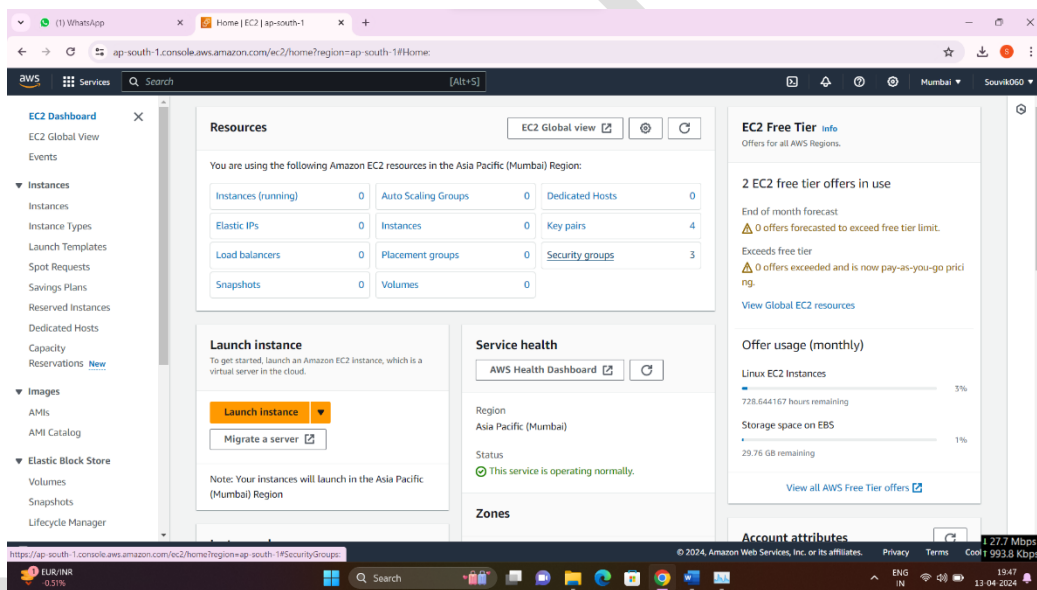
Problem Statement: Deploy a project from GitHub to EC2 by creating a new security group and user data.

Procedure:

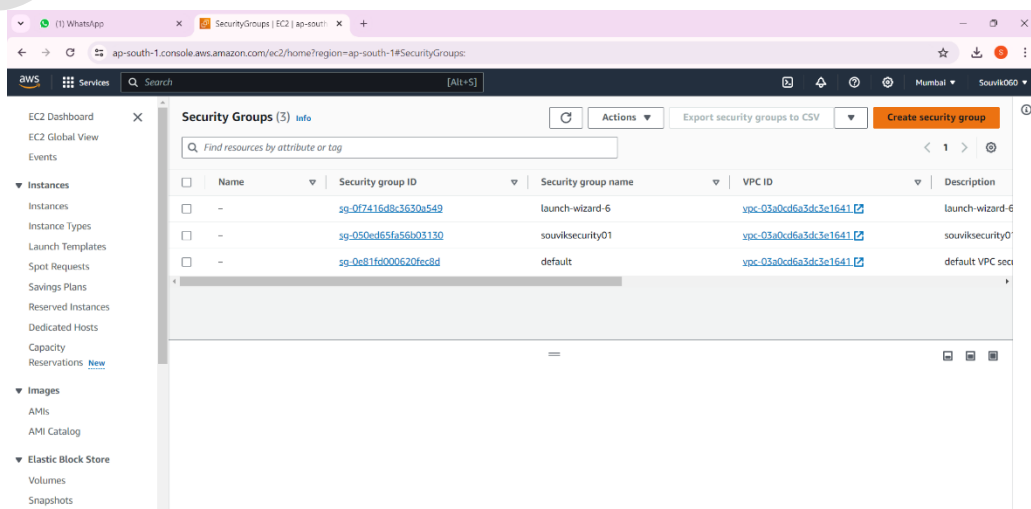
1. Access your AWS console and search for EC2, then proceed to click on the first option.



2. Now, Click on "Security Groups".



3. Now click on "Create security Group".



4. Fill up the name and description (same as name) of the security group.

The screenshot shows the 'Create security group' page in the AWS Management Console. The 'Basic details' section is expanded, showing the following fields:

- Security group name:** SOUSECURITYEC2
- Description:** SOUSECURITYEC2
- VPC:** vpc-03a0cd6a3dc3e1641

The 'Inbound rules' section is currently empty, showing the message: 'This security group has no inbound rules.'

5. Now, scroll down to Inbound Rules and click on “Add rule”. First set the type as Custom TCP, port number as 4000 and select first option in CIDR blocks i.e. “0.0.0.0/0” .

The screenshot shows the 'Inbound rules' section of the 'Create security group' page. A new rule has been added with the following configuration:

Type	Protocol	Port range	Source	Description - optional
Custom TCP	TCP	4000	0.0.0.0/0	

A warning message is displayed below the rule: 'Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.'

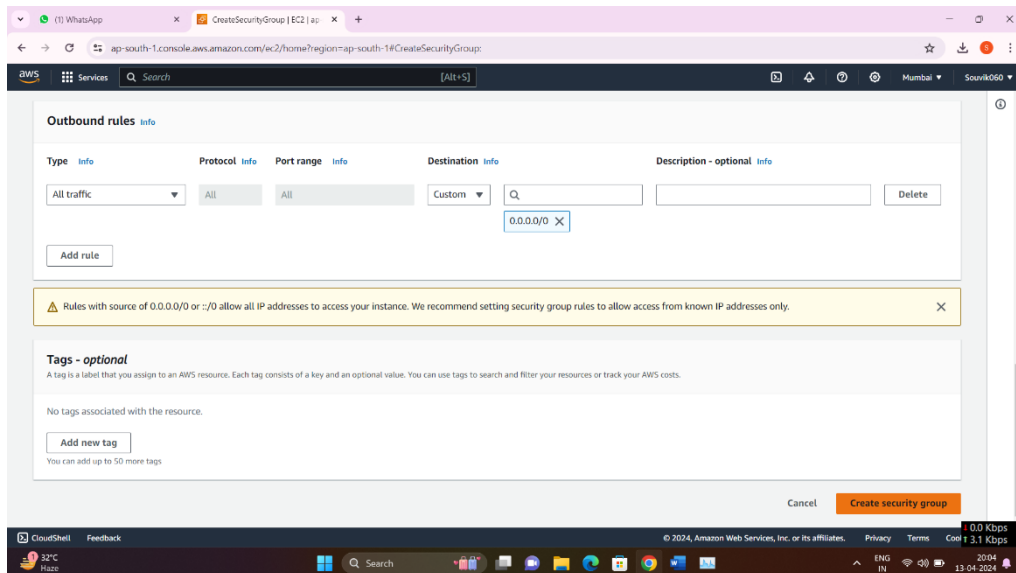
6. Click on “Add rule” again and set type as “SSH” and select first option in CIDR blocks. Repeat this two more times and add rules of type “HTTP” and “HTTPS”.

The screenshot shows the 'Inbound rules' section of the 'Create security group' page. Four rules have been added:

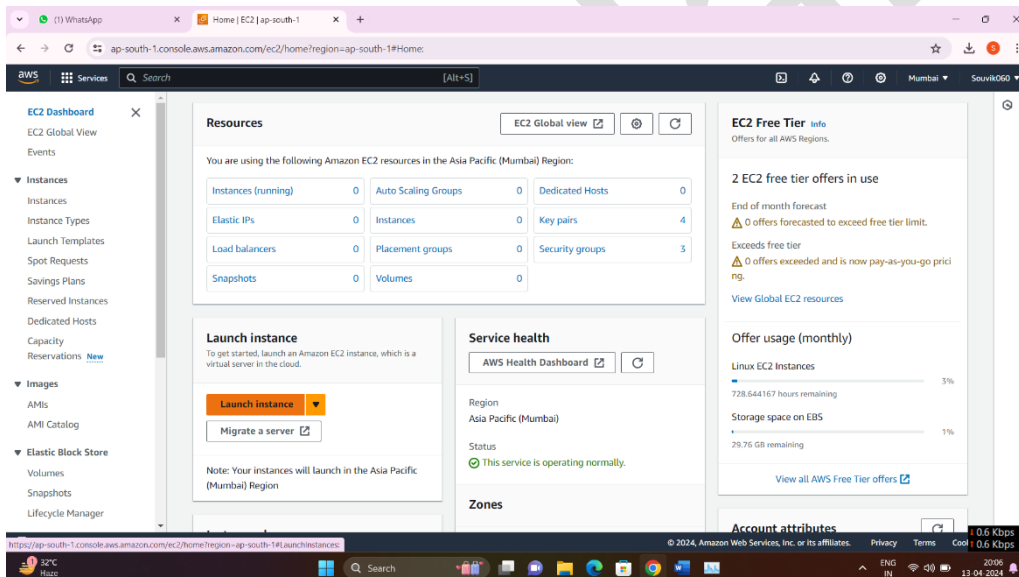
Type	Protocol	Port range	Source	Description - optional
Custom TCP	TCP	4000	0.0.0.0/0	
SSH	TCP	22	0.0.0.0/0	
HTTP	TCP	80	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	

The 'Add rule' button is visible at the bottom of the list. The same warning message about allowing all IP addresses is still present.

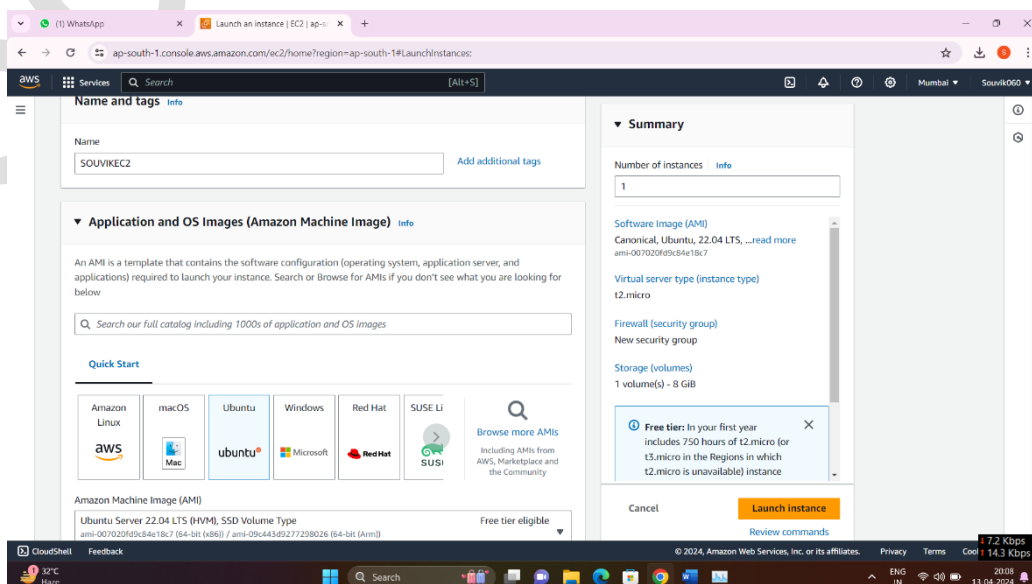
7. Then click on “Create security group”.



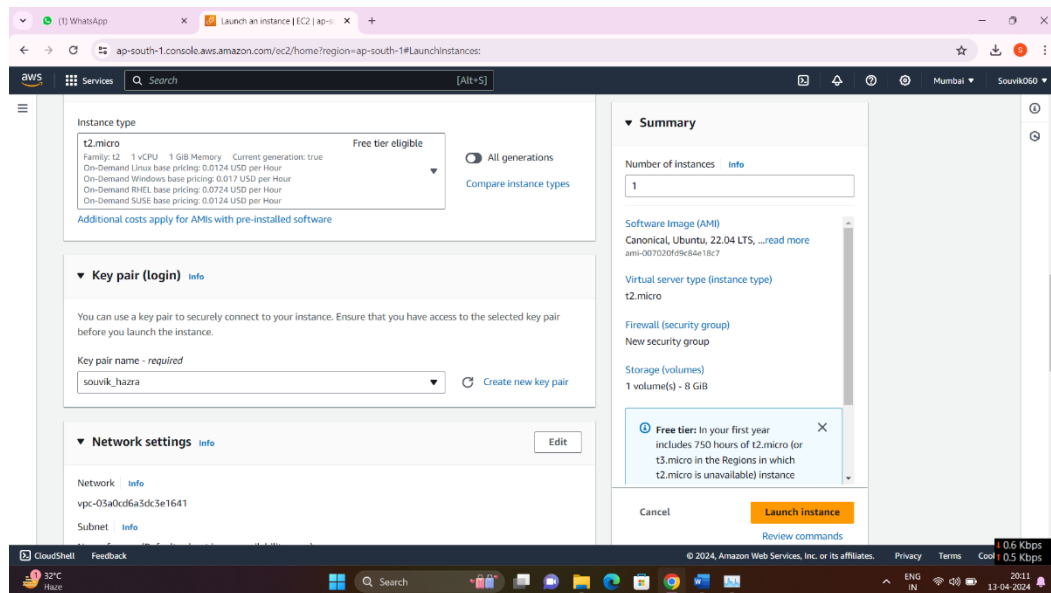
8. Now, go to EC2 dashboard and click on “Launch instance”.



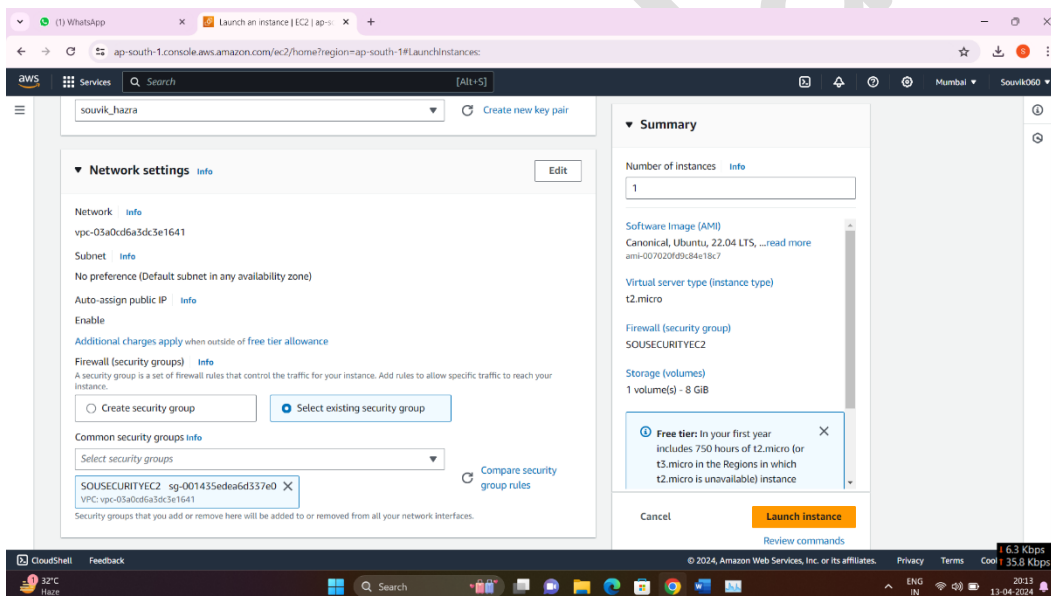
9. Fill up the instance name and select Ubuntu as the AMI.



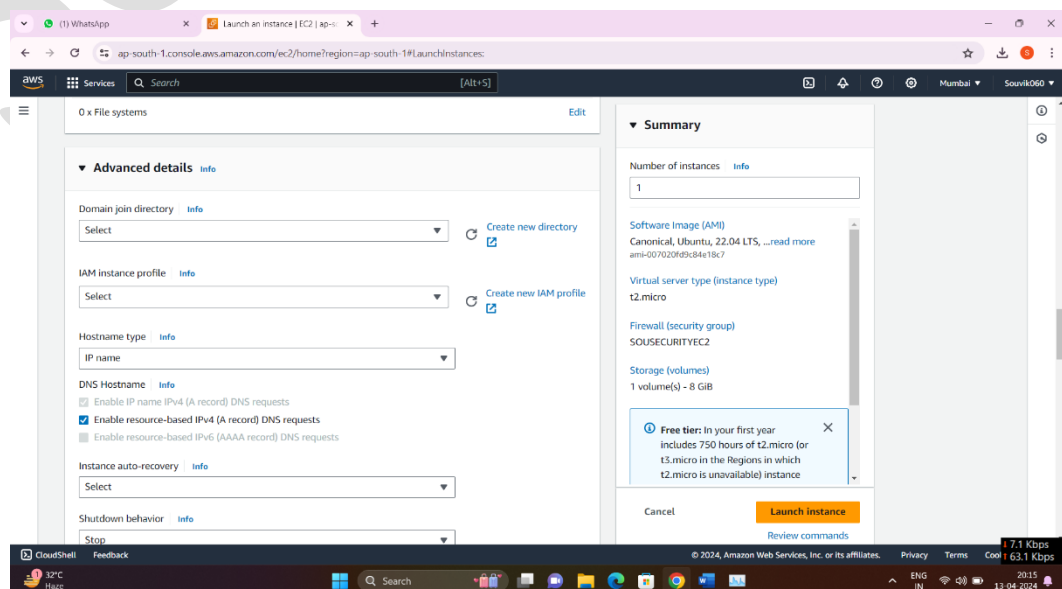
10. Select an existing keypair or create a new one.



11. Now, from Network settings option select “Existing security group” and select the newly created security group.



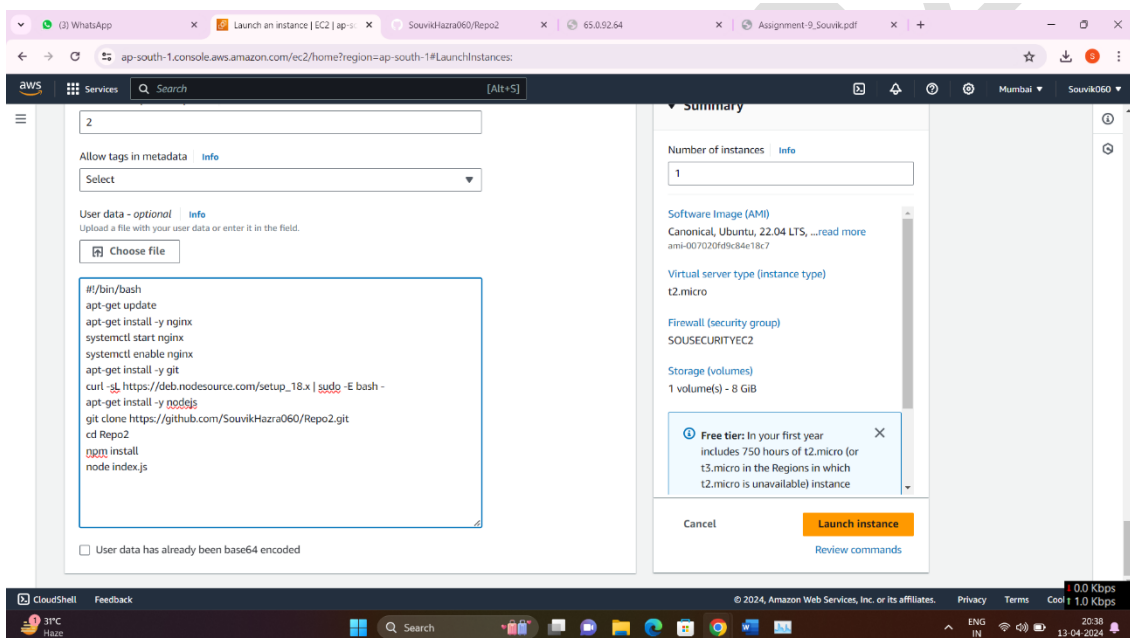
12. Expand the “Advanced details” section.



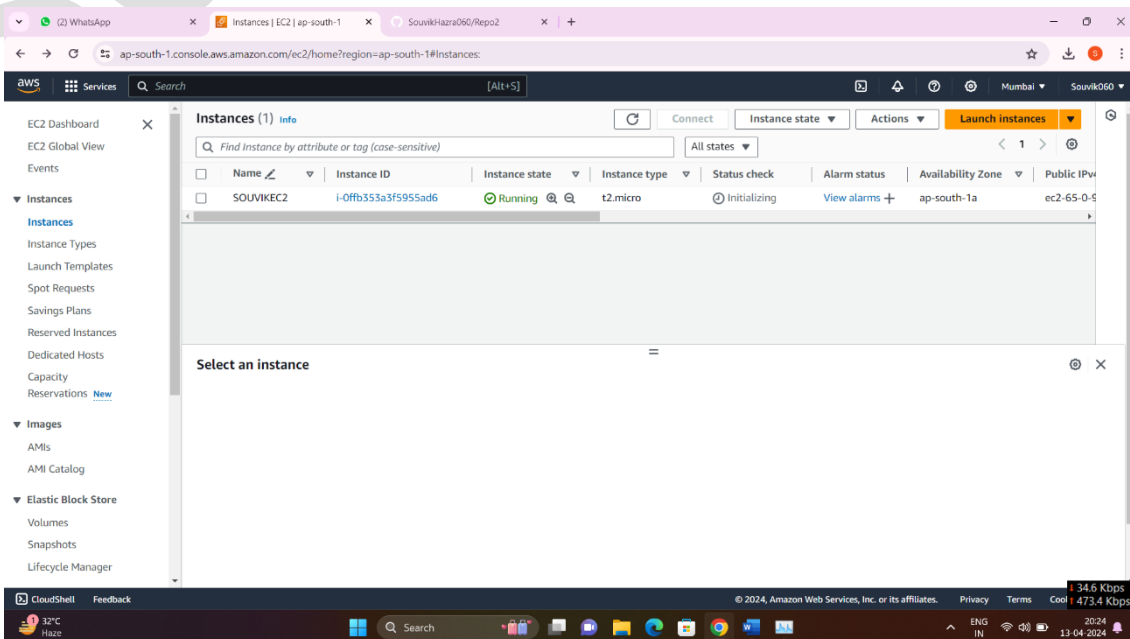
13. Scroll down to the “User data” section and add the following script:

```
#!/bin/bash
apt-get update
apt-get install -y nginx
systemctl start nginx
systemctl enable nginx
apt-get install -y git
curl -sL https://deb.nodesource.com/setup_18.x | sudo -E bash -
apt-get install -y nodejs
git clone <github repository cloning link>
cd Repo
npm install
node index.js
```

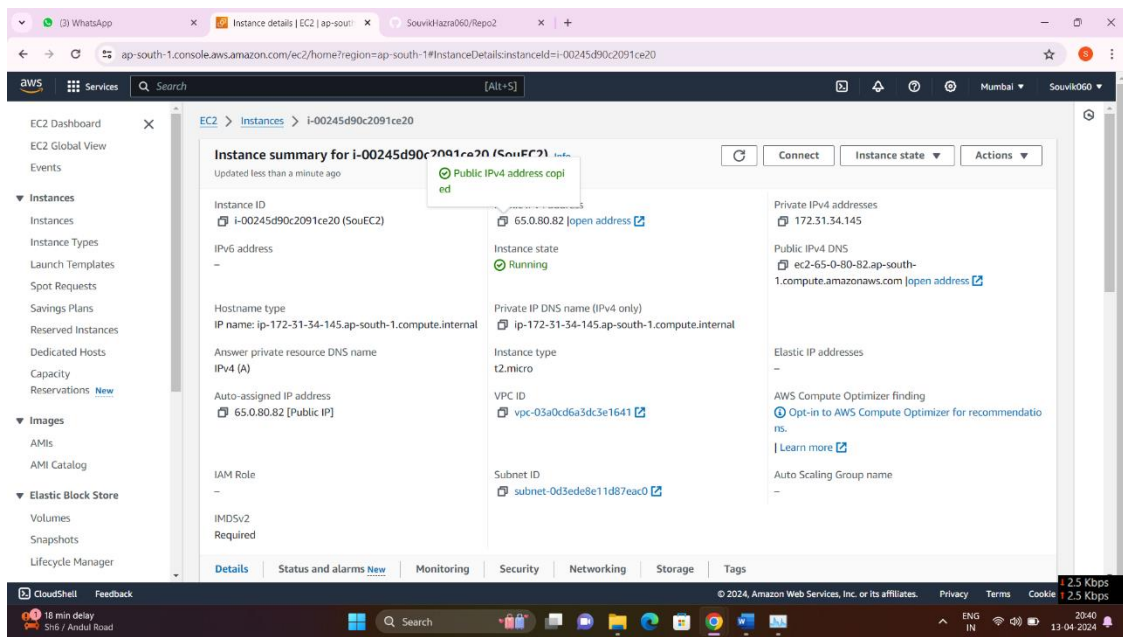
14. Then click on “Launch instance”.



15. Now go to “Instances” and click on the instance id of the newly created instance.



16. Copy the public IPv4 address.



17. Open a new incognito tab and paste the IPv4 address copied then we can see the page “Welcome to nginx!” and add “:4000” to the end of public IPv4 address . This will display our intended website.

