**HPCSA**

Cloud Computing and Security

Lab Assignment 1

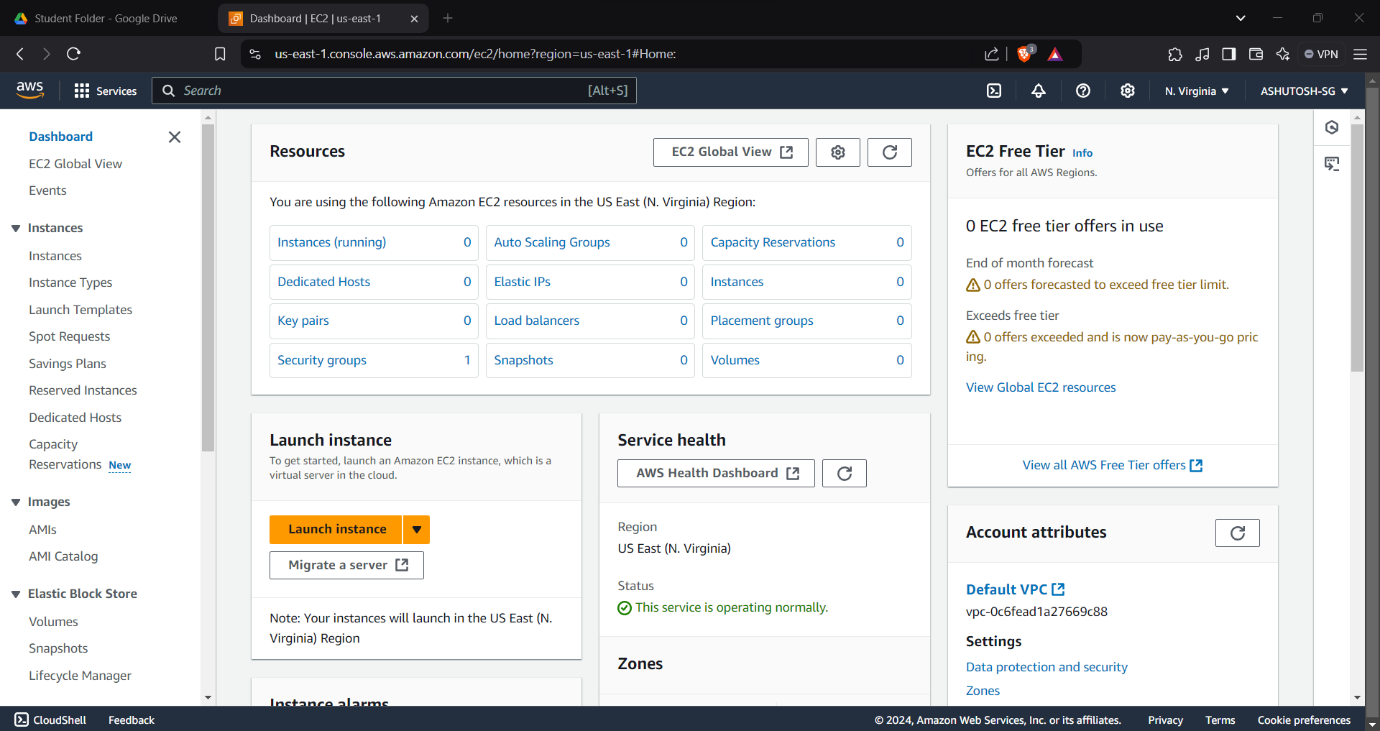
Name : **Ashutosh Gangurde**  
PRN : **240840127031**

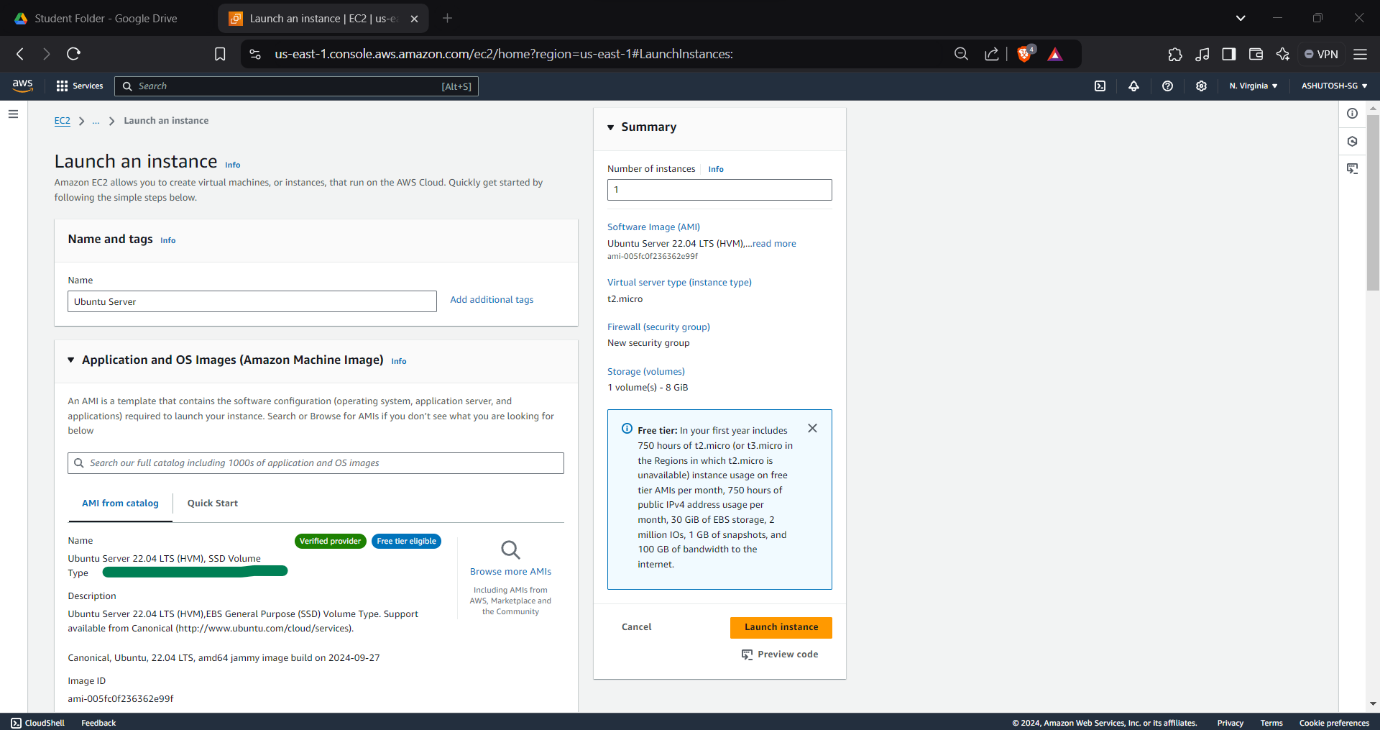
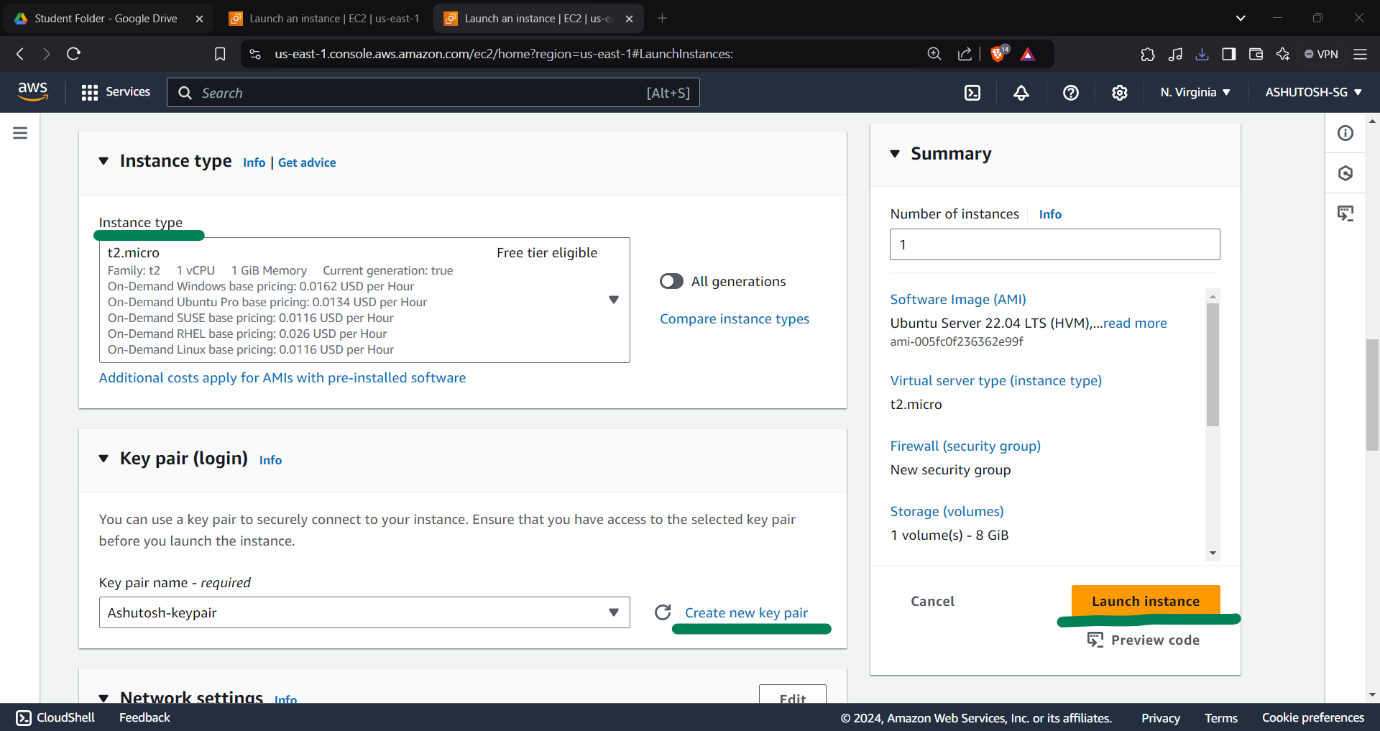
1. Create an Ubuntu EC2 instance and host a website on it which will display “Welcome to Cloud computing” message.

Also copy some files from your machine to this instance using Winscp

**Step 1: Launch an Ubuntu EC2 Instance**

1. Navigate to **EC2** service and click **Launch Instance**.



1. Choose **Ubuntu Server 22.04 LTS** (or the latest LTS version) under the **Amazon Machine Image (AMI)**.  
     
   
2. Select **t2.micro** instance type (eligible for the Free Tier) and click **Next**.
3. Configure the instance as needed and click **Review and Launch**.
4. On the **Key Pair** page, choose an existing key pair or create a new one (download the .pem file as it’s required to access your instance).
5. Click **Launch Instances** and wait until the instance status changes to “running.”  
     
   

**Step 2: Connect to Your EC2 Instance Using PuTTY**

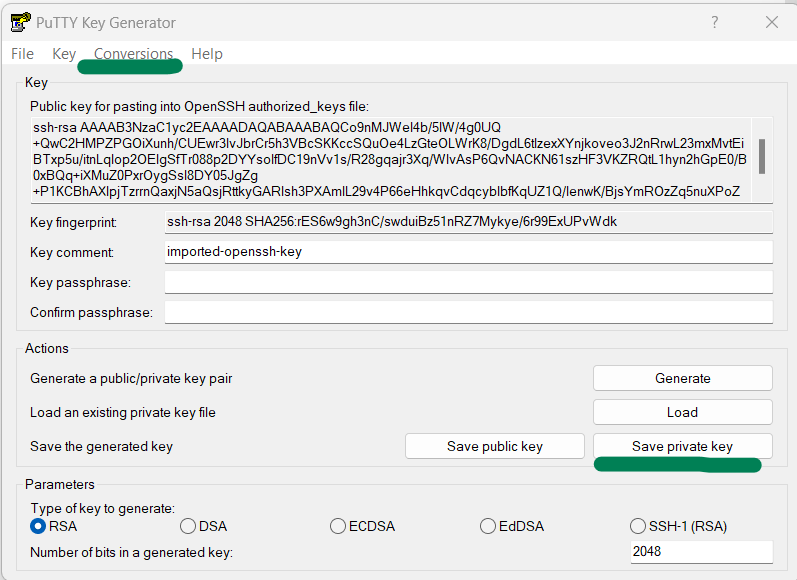
1. Since PuTTY doesn’t accept .pem & Pkt files directly, you’ll first need to convert it to a .ppk format:  
     
   **Convert the .pem Key to .ppk Using PuTTYgen**

Open **PuTTYgen** (part of the PuTTY installation package).

Click **Load** and select your .pem file.

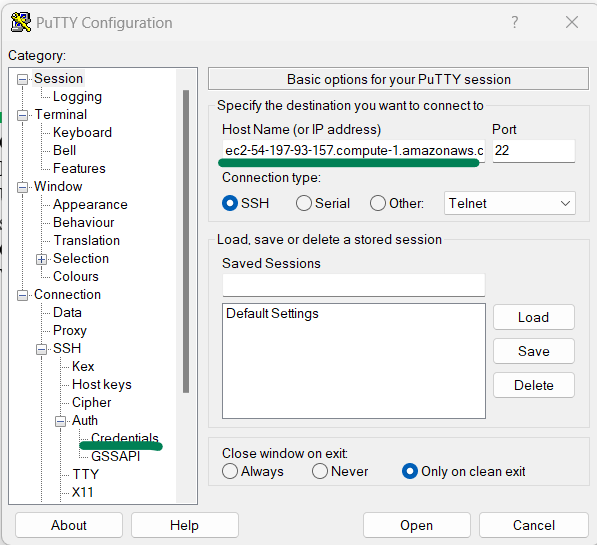
PuTTYgen will load and convert the file. Once it’s done, click **Save private key** (you may get a warning about saving without a passphrase; click **Yes** to proceed).

Save the converted file as a .ppk file.



**Connect to the Instance**

1. Open **PuTTY** and enter your **EC2 instance’s public DNS or IP** in the **Host Name (or IP address)** field.
2. Under **Connection > SSH > Auth**, browse and select the .ppk file you saved.
3. Go back to the **Session** tab and click **Open** to connect.
4. When prompted for the username, enter ubuntu.



**Step 3: Install Apache Web Server**  
  
sudo apt update  
sudo apt install apache2 -y  
sudo systemctl start apache2

sudo systemctl enable apache2

**Step 4: Create a Simple HTML Page**

sudo nano /var/www/html/index.html   
  
<!DOCTYPE html>

<html>

<head>

<title>Welcome Page</title>

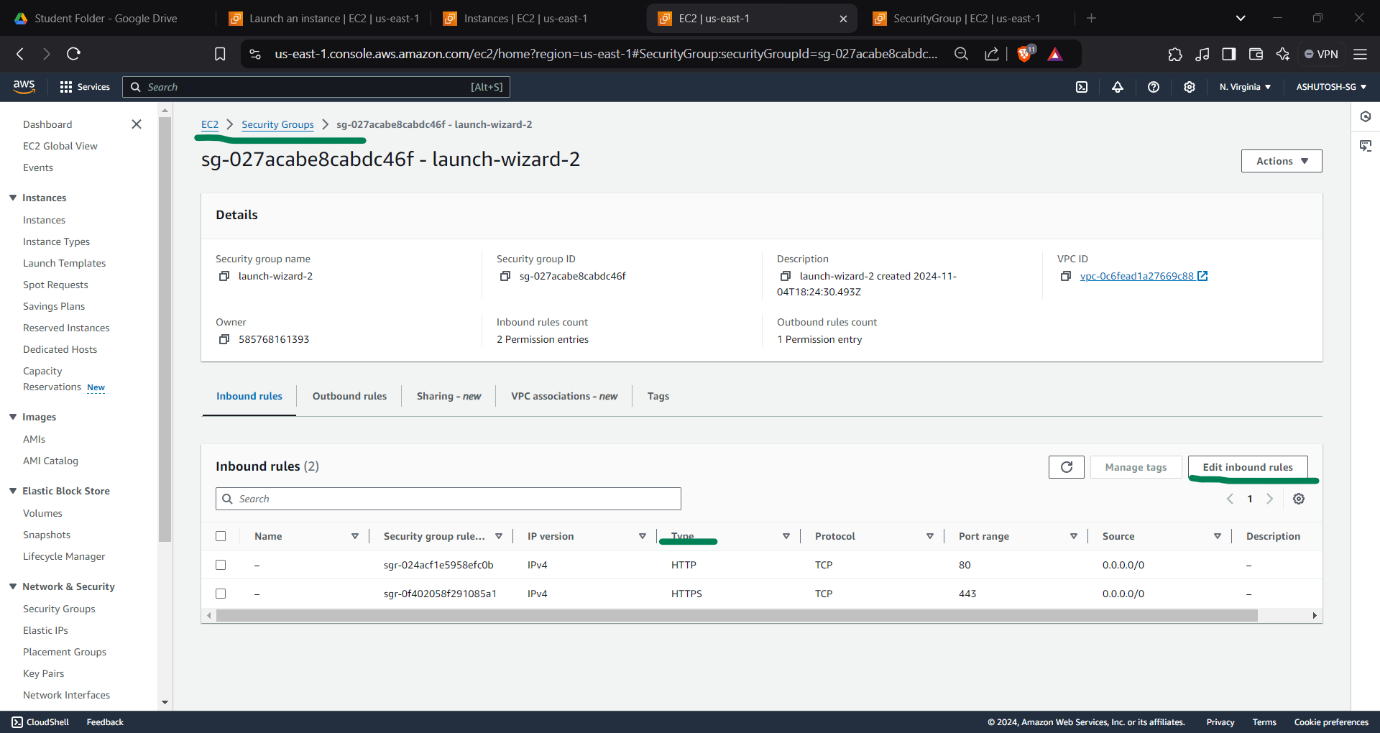
</head>

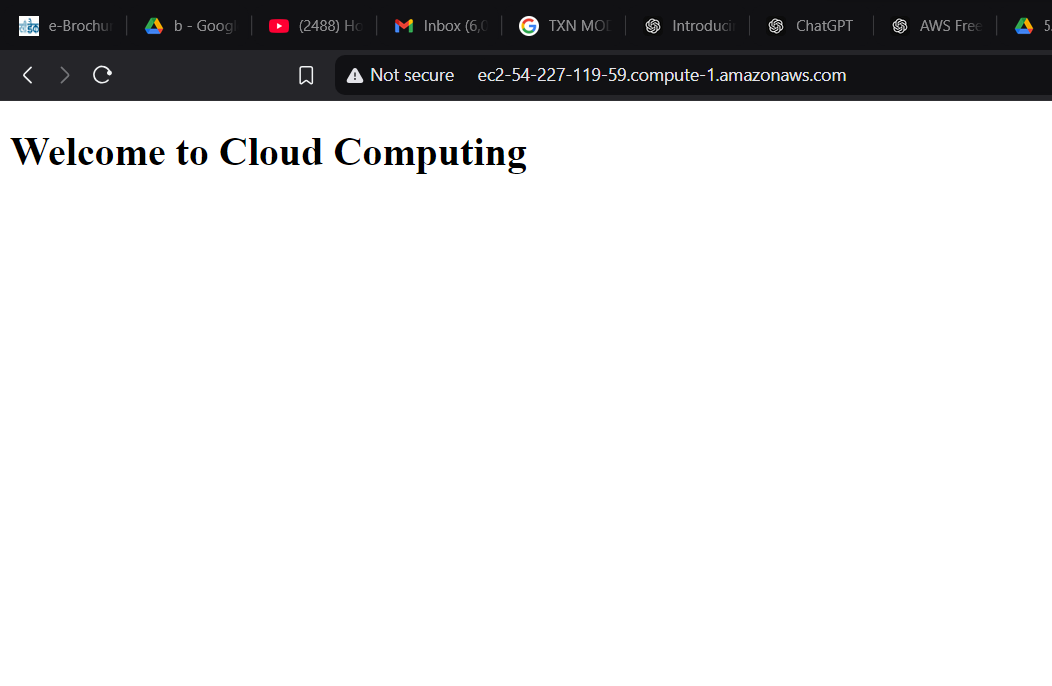
<body>

<h1>Welcome to Cloud Computing</h1>

</body>

</html>  
  
  
**Step 5: Configure Security Group for HTTP Access**

1. In the **EC2 Dashboard**, select your instance.
2. Under **Security**, click the **Security Group** link.
3. Edit inbound rules, adding:
   * **Type**: HTTP
   * **Protocol**: TCP
   * **Port**: 80
   * **Source**: Anywhere (0.0.0.0/0)
4. Save the rule  
     
     
   

Open your instance’s public IP or DNS in a browser to see your message.  
  
  
**Step 7: Transfer Files with WinSCP**

1. Open **WinSCP** and create a new session.
2. Configure the session with:
   * **File Protocol**: SFTP
   * **Host Name**: Your instance’s public IP/DNS
   * **Port Number**: 22
   * **User Name**: ubuntu
   * **Private Key File**: Select your .ppk file.  
       
     **Configure the Private Key File**:
   * Click on **Advanced…** in the bottom left corner of the WinSCP Login window.
   * In the **Advanced Site Settings** dialog, go to **SSH** > **Authentication** on the left sidebar.
   * Under **Authentication parameters**, find **Private key file** and click **Browse…**.
   * Navigate to the location where you saved your **.ppk** file (the converted key from your .pem file).
   * Select the **.ppk** file and click **Open**.
   *  **Save and Connect**:
   * Click **OK** to close the Advanced Site Settings.
   * Optionally, click **Save** on the main WinSCP Login screen to save your settings for future connections.
   * Finally, click **Login** to connect to your EC2 instance
3. Click **Login** and **Yes** if prompted about the host key.

**Verify Security Group Inbound Rules**

Ensure that your EC2 instance’s **Security Group** allows inbound SSH traffic:

* Go to the **EC2 Dashboard** in AWS, select **Instances**, and click on your instance.
* Under **Description**, locate the **Security groups** and click the Security Group ID.
* In **Inbound rules**, make sure there’s an entry for **SSH** with **Port 22** open to **My IP** or **Anywhere (0.0.0.0/0)** (for unrestricted access).
* Save the changes if you added or modified the rule.  
    
  