5. Automate the process of setting up passwordless SSH between two AWS EC2 instances.
Deliverable :- Steps for setting up passwordless SSH

1. Create 2 EC2 instances. We'll refer to them as ec-instance-1 and ec-instance-2.
2. SSH into ec-instance-1 from your desktop using the following command:
   - ➔ ssh -i <path/to/private/key> <user>@<public_dns_of_ec-instance-1>
3. To generate a new RSA key, run the following command:
   - ➔ ssh-keygen -t rsa -N "" -f /home/ubuntu/.ssh/id_rsa
4. Change the permission of your private key by using this command:
   - ➔ chmod 600 ~/.ssh/
5. id_rsa.pub contains the public key. Use cat to view its contents and copy it.
   - ➔ cat id_rsa.pub
6. Now open a new terminal and ssh into ec-instance-2 using the ssh command mentioned in step 2.
7. edit the /etc/ssh/sshd_config file using:
   - ➔ sudo nano /etc/ssh/sshd_config
     now, uncomment the following 2 lines:
     - RSAAuthentcation yes
     - PubkeyAuthentication yes
8. Open the authorized_keys file:
   - ➔ nano ~/.ssh/authorized_keys
     now, append the key you copied from ec-instance-1 by pasting it in a new line. Then save and exit.
9. Change the permission of authoried_keys by using this command:
   - ➔ chmod 755 ~/.ssh/authoried_keys
10. Now, go to terminal where ec-instance-1 was SSHed from and test the connection as follows:
    - ➔ ssh <public_ip_of_ec-instance-2>
11. you can also test the connection by copying files. Use this command to copy files:
    - ➔ scp <filename> <user>@<public_ip_of_ec-instance-2>:/directory