**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

**Set Up SSH Key-Based Authentication Locally:**Generate an SSH key pair and configure it for passwordless login between two local machines or VMs.

Name: Sivakumar C Department: AML



**Introduction**

Securely accessing remote servers without repeatedly entering passwords is essential for efficient system management. SSH key-based authentication provides a more secure and convenient method compared to password authentication. This document outlines the steps to set up passwordless SSH login between a local machine and a virtual machine (VM).

**Objectives**

* Generate an SSH key pair for authentication.
* Configure the remote VM to allow passwordless login.
* Establish a secure and efficient SSH connection without using password authentication.
* Improve security by eliminating password-based access.

**Importance**

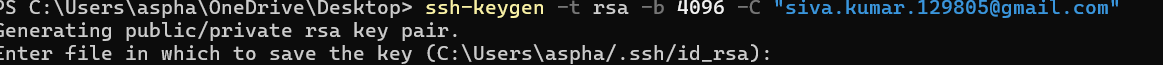
* **Security:** SSH key authentication is more secure than passwords, reducing the risk of brute-force attacks.
* **Convenience:** Eliminates the need to enter passwords every time you connect.
* **Efficiency:** Enables automated and seamless remote access to systems.
* **Best Practice:** Following industry-standard security measures ensures robust access management.

**STEPS:**

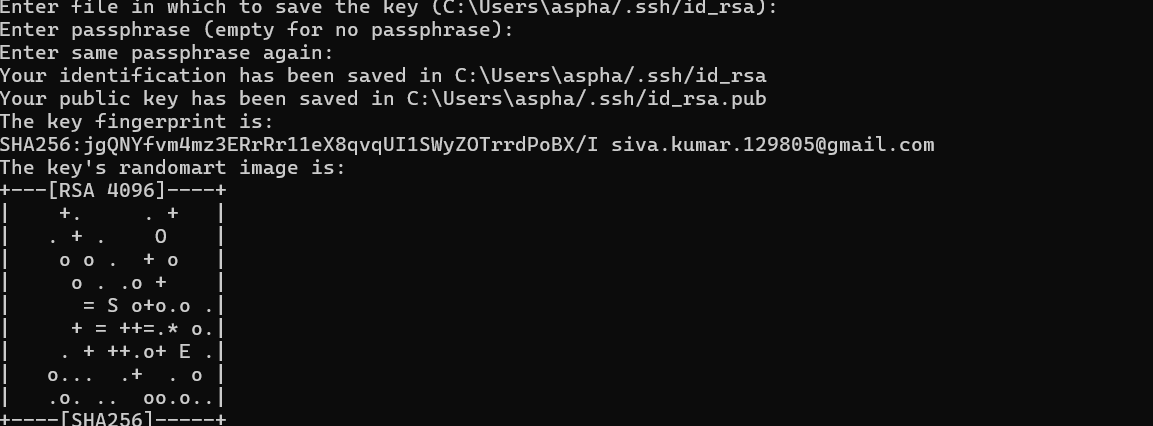
**STEP 1:** **Generate an SSH Key Pair on the Local Machine**

Open a terminal on your local machine and run the following command to generate an SSH key pair:

**ssh-keygen -t rsa -b 4096**

****

Press **Enter** to save the key in the default location (~/.ssh/id\_rsa). When prompted for a passphrase, you can leave it blank or set one for additional security.



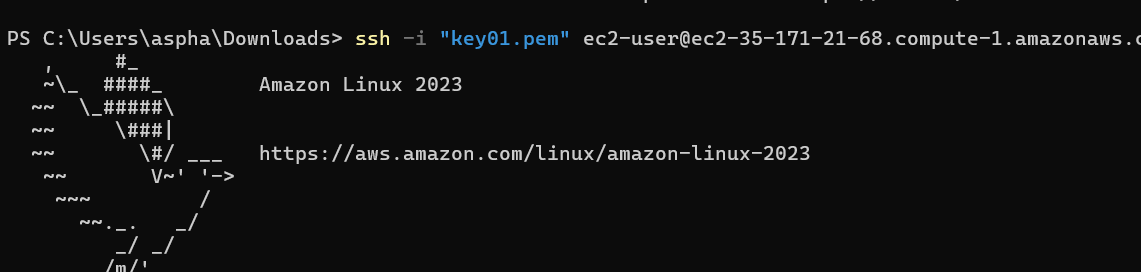
**STEP 2: Copy the Public Key to the Remote VM**

* Open Notepad on your local machine and navigate to the SSH key directory:

**notepad %USERPROFILE%\.ssh\id\_rsa.pub**

* Copy the entire contents of the public key (id\_rsa.pub).
* Open a terminal and connect to your VM using SSH with the .pem key file:

**ssh -i your-key.pem ec2-user@your-vm-ip**

****

**STEP 3:Paste the key into the ssh directory**

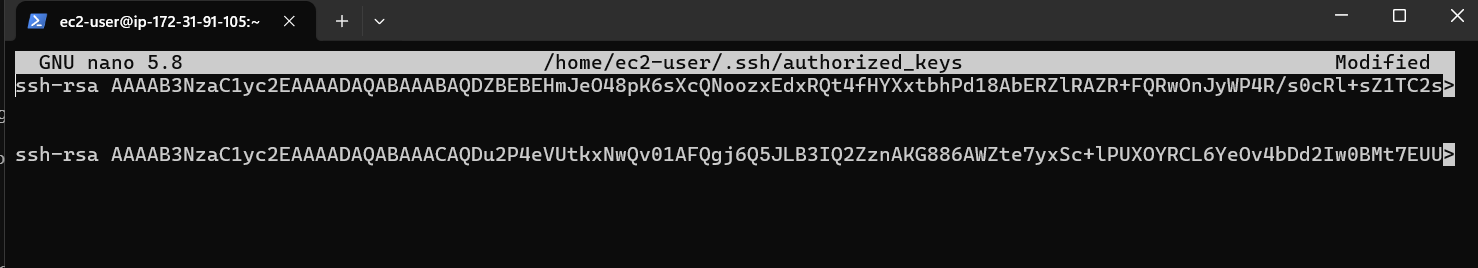
* Once inside the VM, create the .ssh directory if it doesn’t exist:

**mkdir -p ~/.ssh**

* Open the authorized\_keys file using nano:

**nano ~/.ssh/authorized\_keys**

* Paste the copied public key into the file, then save and exit **(CTRL+X, then Y, and Enter).**



* Ensure the correct permissions are set:

**chmod 600 ~/.ssh/authorized\_keys**

**chmod 700 ~/.ssh**

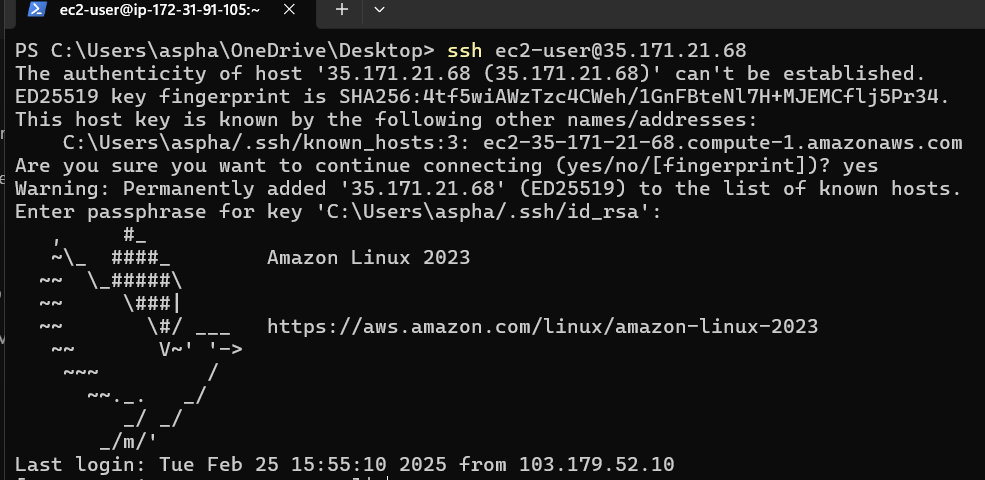
****

****

**STEP 4: Connect to the VM Without a Password**

Exit the current SSH session and attempt to log in again using the newly configured key-based authentication:

**ssh ec2-user@your-vm-ip**

****

If everything is set up correctly, you should be able to access the VM without using the .pem key file or a password.