How to Securely Access Application or Database Server in a private Subnet using Bastion host without using aws management console.

- **Select a Region**
  - "us-east-1, us-east-2, us-west-1, us-west-2"
- **Create a vpc**
  - CSD-vpc, Cidir block = 10.0.0.0/16
- **2 subnet; one public & one private**
  - CSD-pub-sbn, Cidir block = 10.0.0.0/24
  - CSD-prv-sbn, Cidir block = 10.0.1.0/24
- **Create 2 route table and configure it by routing the traffic and subnet association**
  - CSD-pub-RT, CSD-pub-RT
- **Enable DNS hostname**
- **Create an internet gateway**
  - CSD-igw
- **Create a Bastion host server in the public subnet**
  - open only port 22 @ the level of the S.G and traffic from anywhere or your IP
- **Create an Application or Database server in the private Subnet (make sure traffic only comes from the Bastion host server to your private subnet)**
- **SSH into the Bastion host server and through your bastion host server ssh into you Application or Database server in your private subnet)**
  - 'mkdir call it mycred, cd into mycred,
  - create a keypair file { vi mykp.pem)
  - Escalate the Key pair (chmod 400 mykp.pem)

  - **SSH into the AppDB server using mykp.pem**
    - { ssh -'i "mykp.pem" ec2-user@AppDBPrvIP **}**

AWS Cloud

Region

VPC

Haz-1

Pub. Sub-1

NAT Gateway

Bastion host server

Amazon **EC2**

Prv. Sub-1

Amazon **EC2**

Haz-2

Pub. Sub-2

Bastion host server

Amazon **EC2**

NAT Gateway

Prv. Sub-2

Amazon **EC2**