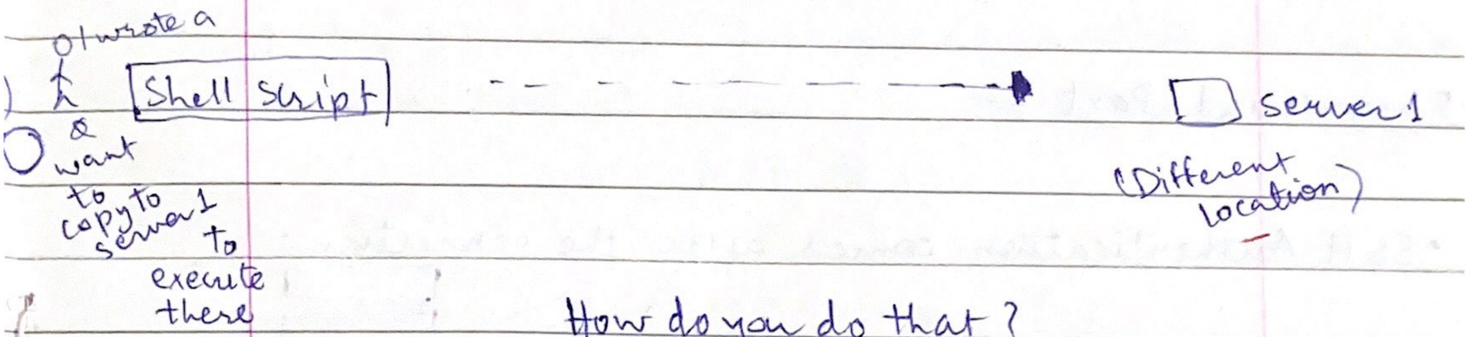
SSH

- Secure Shell.



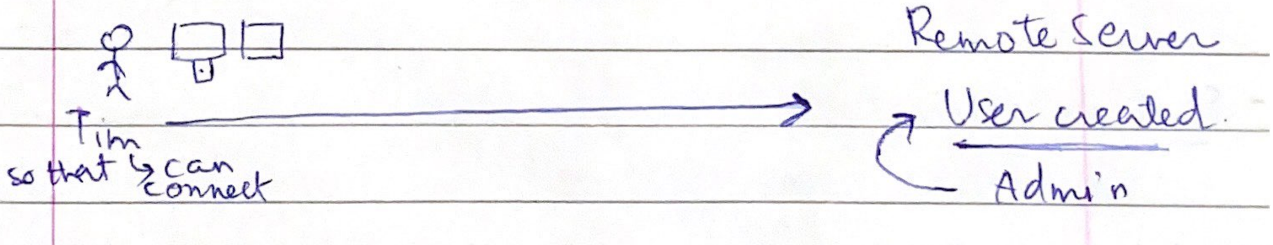
How do you do that?

- SSH

- accesing a machine over internet.
- want to connect to it securely.

Two ways of authentication.

(1) Username & Password.



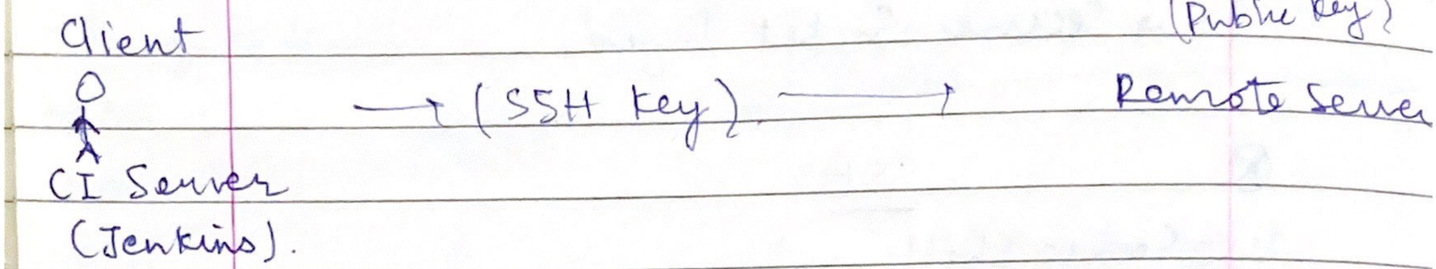
(2) SSH key pair

Client machine - (Private key)

create SSH key pair (encrypted) | needs to store securely.

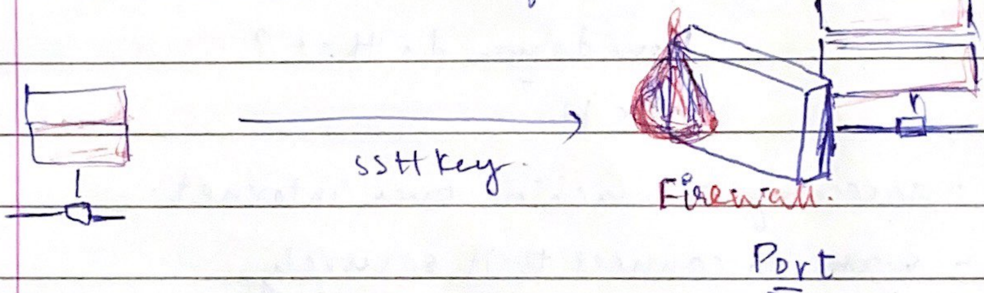
Remote (public key)

• SSH for Services



• Firewall and Port 22

• SSH Authentication comes after the connection.



what port?

• Always listen to port 22.

• needs to be restricted to specifi IP addresses

- SSH in action

Cloud linux: IP Address.

• Connect via IPV4. In our linux machine:

```
ssh root@IPV4
     ↓
  password.
     ✓
```

User home directory

.SSH/ Folder

Page

Date

Cryptographic Algorithm
↓

• Ssh-keygen -t rsa : To create the key.

~/.ssh → default location

passphrase → for additional Security.

id-rsa   id-pub

↓ private key   ↘ public ~~private~~ key (shared with the remote server)

list of publickeys - no. of people want to join.

In server: ls .ssh → authoriced keys

• copy public key and paste to remote Server → authorized keys file.

- .ssh/id-rsa → default location ssh will look for private key.

or ssh -i .ssh/id-rsa root@IPV4

- can have multiple groups.

```
sudo usermod -G admin username
```

↑ overrides.

```
-aG newgroup
```

↓ append

copy bash script and Execute

```
- scp test.sh root@IPV4:/root
```

→ secure copy

```
scp -i .ssh/id_rsa file root@IPV4:/ 
```

dest. location

↑ location

Now, we don't need to provide password

-Because the private key was used to authenticate

* known-hosts

lets client authenticate the server to check that it isn't connecting to impersonator

* authorized-keys

· lets the server authenticate the user.

- we see, we don't provide private key. But why? How does it work?

```
.ssh/id_rsa
```

↑ default location for private key search.

So - ssh -i location of private key root@IPV4.