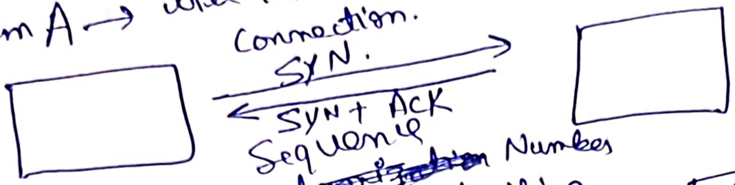
Session6: Imp Topics SSh & IAM Roles

Prootocols (TCP & UDP).

Laptop-Browser

System A → will initiate the connection.

Client



SYN. →

← SYN + ACK

Sequence ~~Synchronization~~ Numbers

S/NO ⇒ Anything (8000).

↓

Random Value

B (Server (Google, Instagram etc).

(24x7). (10MB)

↳

→ Segments.

Port No 22 ⇒ SSh

Browser ⇒ 80

Port No		80
(MSS) Maximum Segment Size		P.No

(1Kb). (1024 Byte)

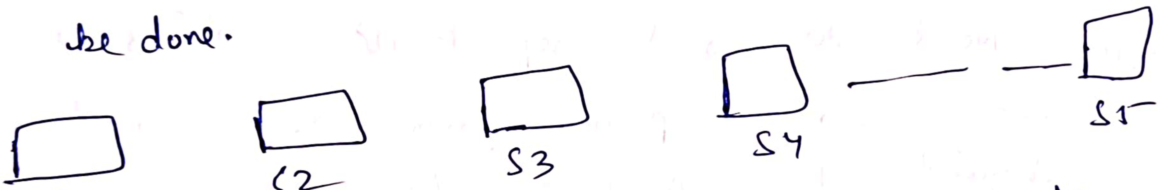
TCP Header.

Client will sent to Server. → Connection establishment step.

Synchronization flag (0/1). (1) for our Port No.

TCP Header.

→ Once connection is established then only Data Transfer will be done.



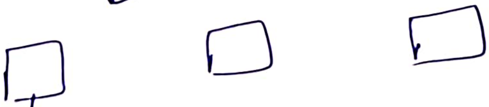
S1 Unique Identifier (Sequence No)

② Source Server

Destination (my laptop) Request.

80	Port A
Seq ⇒ 3000	
Ack ⇒ 8000+1 ⇒ 8001	

→ Server has acknowledge the Request

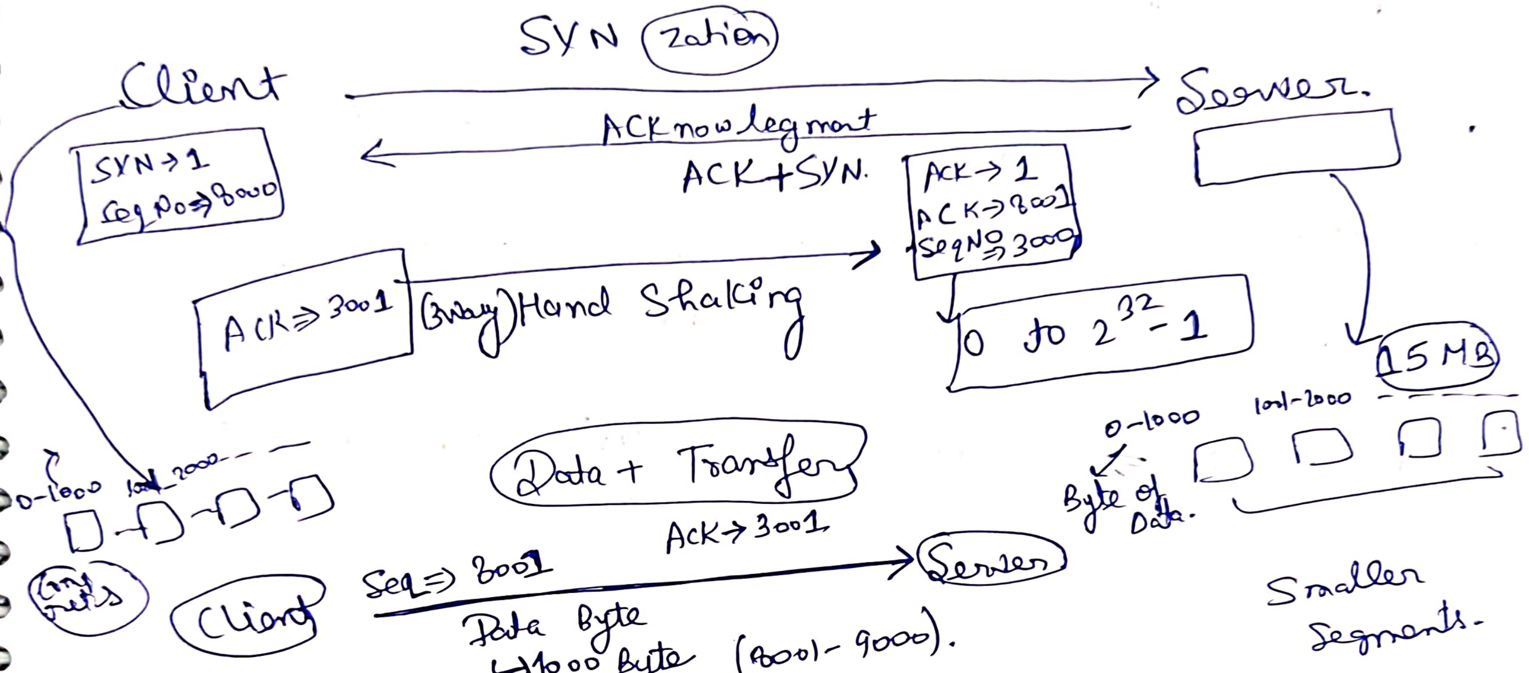


3000 (Unique Sequence No).

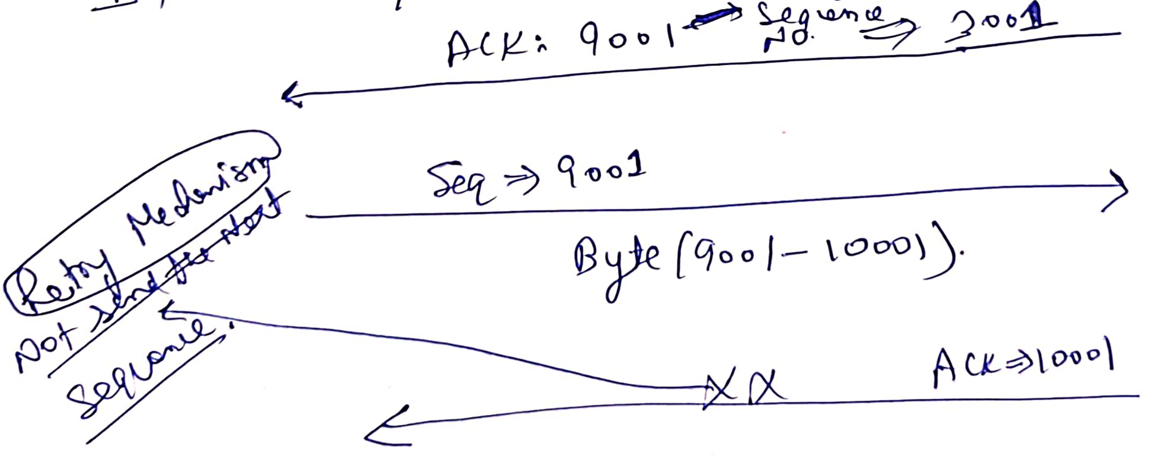
(3) (Three way Hand Shaking).
3-Way

ACK ⇒ 3001
Ack flag ⇒ 1

New Diagram

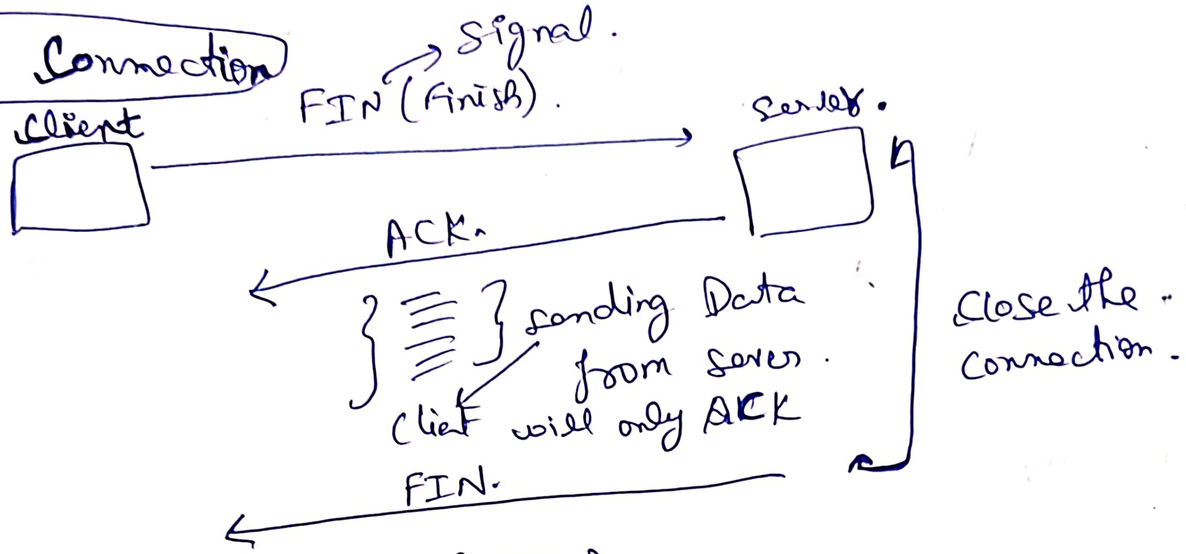


In one Segment transfer only 1KB of Data


ACK: 9001 → Sequence NO. ⇒ 3001
Seq ⇒ 9001
Byte (9001-10001).
Retry Mechanism
Not ~~send the~~ next sequence.
XX
ACK⇒10001

⇒ Closing the Connection once Data Transfer is Complete.

Close Connection



.(4-Way Handshaking).

2:> **Drawback of TCP:->**

Sequence No will be Given By Browser/ Kernel

As ACK the Request everytime, so it is always slow. therfore will be using UDP Protocol.

TCP Header => Exchange the Info B/w Client & Server.

UDP ⇒ whatsapp

Chat

TCP

Video Call

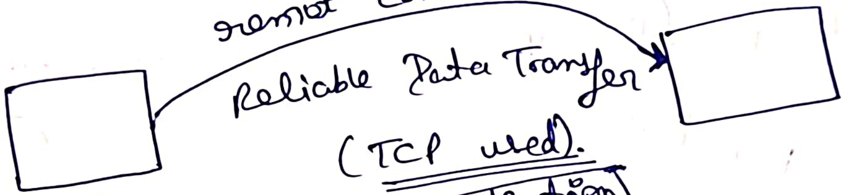
Reliability is not that Imp. (Data Transfer fast : UDP).

→ Photo being Captured.

→ Used in all services, where streaming is being used. (Speed is more Important).

(Direct Data Transfer will Happen).

⇒ SSH



(TCP used).

laptop → Anypart in this world. Wants to access ec2-instance.

Authentication

~~Password Based~~ → Disabled

Key based → Password less login

Asymmetric encryption.

Public Key

Private Key

RSA Algo

Public → encryt data.

Private → Can only decrypt data.

Practical . Launch an instance.

⇒ Two (2) kinds of Authentication.

⇒ Will always do a remote login

Private Key

launch 2 instances to communicate to each other.

Key Based login

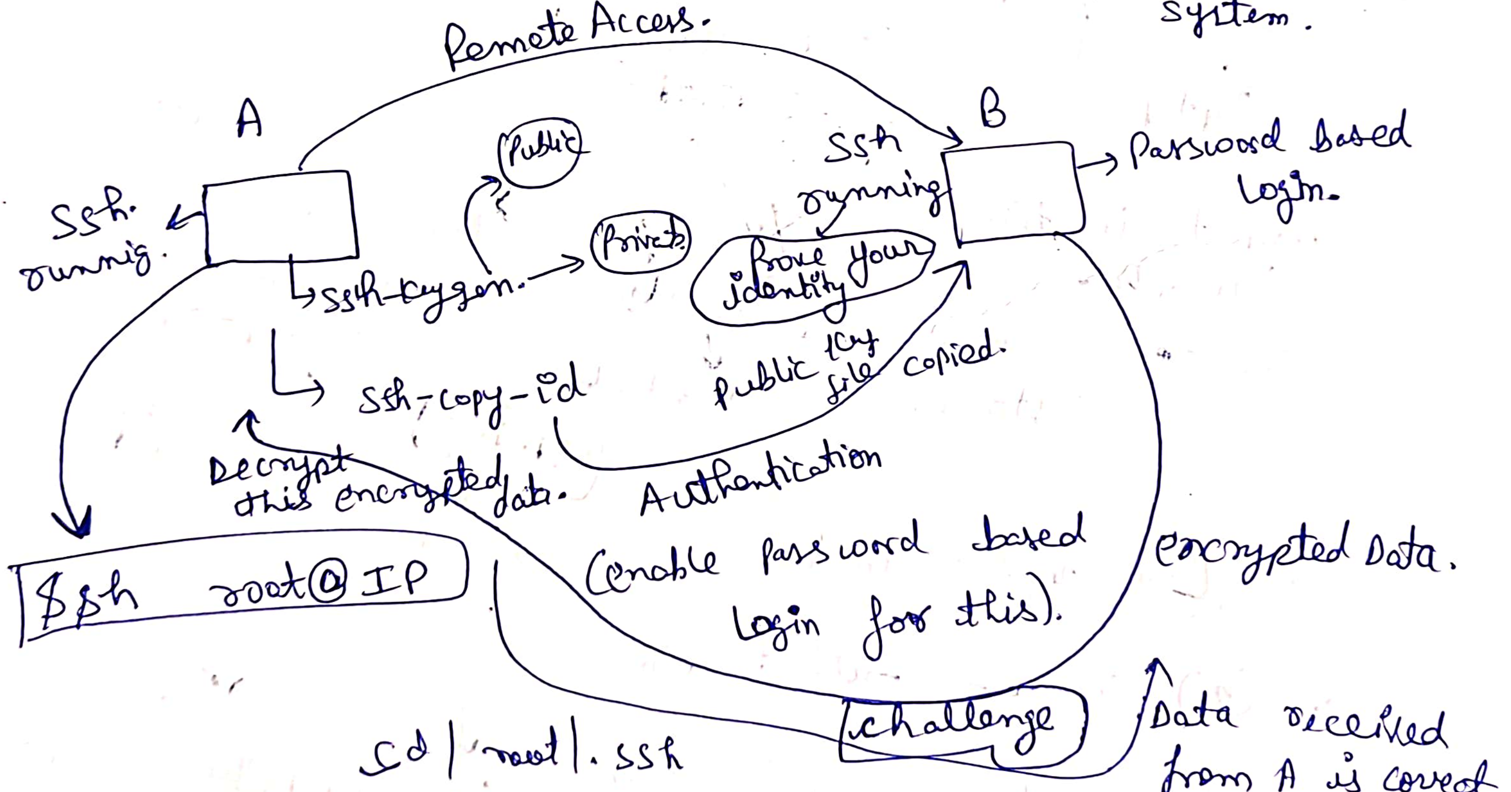
RSA Algo to create a set of Key Pair

⇒ `ssh-keygen -t rsa`

- Publi / Private key will also be in pairs.

⇒ copy keys from one system to another.

ssh-copy-id -i Path of key ⟹ ip address. of another remote system.



cd /root/.ssh

⇓

Authorized keys

- Public key ⇒ encryption.
- Private key ⇒ Decryption.

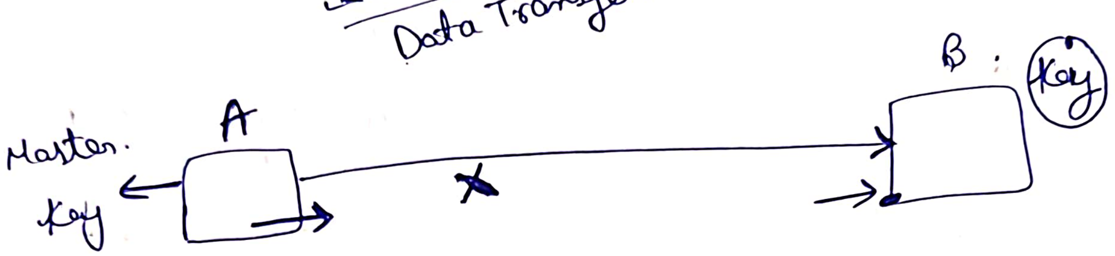
→ Behind the scene (Keys are being used)

Data Transfer ⇒ Symmetric Key → Encryption
→ Decryption.

Use both Symmetric & Asymmetric.

↙ Communication
Data Transfer.

↓ Authentication.



Cipher Text Data Transfer ⇒ Integrity of Data
(Should not be Modified).

① . Confidentiality → encrypt

② Integrity of data → Hashing.

③ Authentication → Decrypt

Great Algorithm is
Diffie-Hellman
Key exchange
to create
Master Key

→ Hello → convert into a very big string
(Hash value)
. Unique hash value.

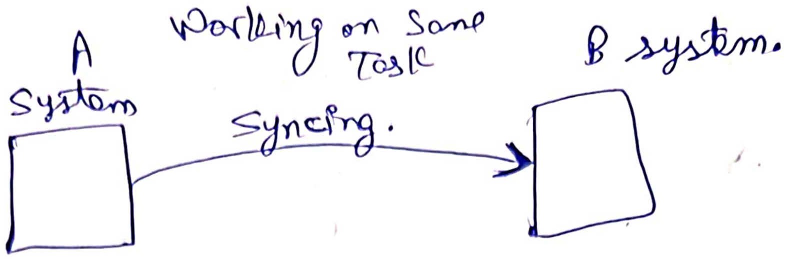
⇒ echo Hello | sh

list of Algos.

echo Hello | sha512hmac
↓

Hash value length will always be same.

Imp Topic



Data Generated

Program: rsync

A

mkdir data

⇓

cd ./data

⇓

touch a.txt etc.

B

mkdir backup

⇓

cd backup

-av → verbose

rsync A/data root@123.4-6.7:/backup.

other System IP

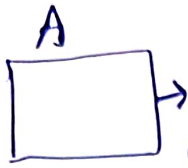
- will use ssh protocol behind the scenes.

from B as well, Permission / other Meta data Information is also copied.

Pblm: Running rsync manually is not Good.

run a program in A at regular intervals.

Cronjob



→ Backup command

↳ Everyday at 12 AM
automatically
/every hour.

⇒ Install

Crontab
⇓
yum whatprovides crontab
⇓
yum install cronie
⇓ installed.

Systemctl start crond → unit file Name.

Crontab -l ⇒ How many cron jobs are created

⇒ man crontab. (list)

⇒ crontab -e (file).

⇓

In this file do this schedule
↳ website.
Crontab guru

~~* * * * *~~ rSync
Command.

folder ⇒ Compressed the folder then cp.

⇒ tar --help ⇒ ~~tar -cvz~~.

⇒ tar -czvf backupgfg.tar.gz /gfg/

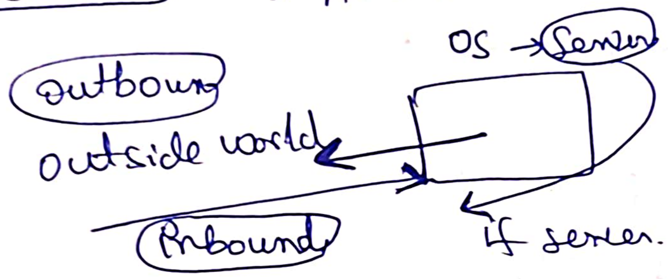
CP filename /data/

↳ Because in this cron is running.

extract

⇒ tar -xvzf filename.

Firewalls → System
→ AWS security group.



Every OS have their own firewall

AWS → Security Group

⇒ Install firewalld

⇓

Now installed. (will not start the service)

⇓

Install httpd (Apacha server).

⇓

Systemctl start httpd.

⇒ rpm -q firewalld.

⇓

systemctl status firewalld.

Security Group ⇒ ALL,

Systemctl start firewalld ↓ browser keeps on trying.

⇒ Inbound Have not allowed from internall firewall

How can we manage Inbound/out bound in Internal fire wall.

⇒ firewall-cmd --list-all ↓ want to allow http service as well.

⇒ firewall-cmd --get-services | grep http.

⇒ firewall-cmd --add-service http.
↳ allowing http traffic

⇒ vi /etc/httpd/conf/http.conf ↓ By defaullt works on 82 port.

⇓

Systemctl restart httpd.

⇓

change/add rule to allow P.No 82.

⇓

firewall-cmd --add-port 82/tcp ↓ success response.

Problem Rules adding rules adding are not Permanent.

⇒ firewall-cmd --reload.

⇓

firewall-cmd

Remove some rules

--add ⇒ --remove

↓

reload firewall-cmd --reload.

* I wanted to allow/reject a particular IP/Person

cat /var/log/httpd/access_log]

from this IP Address hacker to connect My system

Blocked the IP.

```
firewall-cmd --add-rich-rule='rule family = "ipv4"
                 Source address = "____"
                 reject'
```

Range of IP Address

CIDR (Notation)

Outbound Traffic Ping 8.8.8.8. I By default have a connectivity.

```
firewall-cmd --direct --add-rule ipv4 filter OUTPUT 0 -d
                                  8.8.8.8 -j DROP.
```

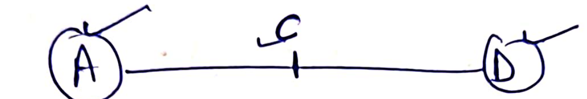
*Not permanent.

Can add priority to rules as well

0 → most priority
1 → less
↓ less.

Allow

(i)



(IP Address) (IP Address Range)

(ii)
outside IP Address
↳C→ Drop the Packet.
↳C→ Drop x.

* firewall will go to least priveleges