1) Backend deployment
2) Problems Faced
3) React JS
4) DSA

Back-End Development

Backend – Learn What Matters Part 1 – Sheryians Coding School

1) Internet
   How data is transmitted through internet across different countries:
   When a message (data) is send through internet, it travels to the nearest tower in the form of packets. The packet cannot travel for long distances, when it does it gets an error.
   The tower transmits the message through wires under the sea, to the nearest tower of the destination.
   The tower now converts the signal into the packets, which is transmitted to the destination.

   How data is transmitted through internet within a country:
   When a message (data) is send through internet, it travels to the nearest tower in the form of packets. The packet cannot travel for long distances, when it does it gets an error.
   The tower transmits it to the ISP, checks if it is valid or not, if it is then, it is transmitted to the nearest tower of the destination.
   The tower sends the packets to the destination.

   Raw figure of internet
   Connecting different countries through optical fibers to transmit data
   PHONE – packet --→ TOWER – electric signal --→ OPTICAL FIBERS --→ electric signal -- → TOWER – packet -- → PHONE

   Who owns internet: Noone

2) Router:
   Receives signal from the connected device and forwards it to the internet.
   Forwards the received signal to the connected device by checking the MAC address. For example, a phone P1 with MAC address abcd is connected to the router, when the router receives a message which is to be forwarded to the phone P1. It forwards it using the MAC address.

   In old days, the WhatsApp used to get hacked by:
   A hacker would change the MAC address, due to which the message to be transmitted from the router gets forwarded to two devices (hacker's device) and the destination device with same MAC addresses.
   End to end encryption prevented such hacking. Even if the MAC addresses were same and the message would be forwarded to both the devices, the device would receive encrypted message, so in order to read the message, one needs to decrypt it. To decrypt the message, a secret key is required which is stored in the device. So, the hacker's device could not access the encryption key and hence could not get access to message.

3) Server
Any computer or software connected to a internet and is programmed to receive request and provide responses is server. It needs to be turned on and connected to internet all the time.
Various types of servers: web servers, email servers, file servers, database servers.
A server can be used as a normal computer as well. But it is not done as upon doing so, the computational power gets distributed and the capacity of server is reduced. In order to maximize the computational power of the server, it is dedicated to perform specific tasks only. The devices such as monitor, mouse, keyboard are removed and only a processor is kept.

CLIENT –request –→ SERVER – response -- → CLIENT

4) Client
Who sends request to the server.

5) http and https
the only protocol(s) on which data can be exchanged, internet can be surfed.
Set of rules to be followed on internet to exchange data and surf internet.

http: unsecured
Hyper Text Transfer Protocol
When a computer sends message using http website, the message can be accessed by hackers.
Doesn't encrypt data.
Don't provide information on unsecured websites(http)

https: secured.
Hyper Text Transfer Protocol secured.
When a computer sends message using https website, the message can be accessed by hackers but the message won't be readable as the message is encrypted. It gets decrypted only on the server.
Encrypts data.

6) Ports
Random numbers
Four to five digits
When some device is connected to the port, it can not be used by others.

Closed ports:
Through the closed port, a device can be connected to the server.

Opened ports:
Through the opened port, a device can be connected to the server.

7) ISP
Internet provider