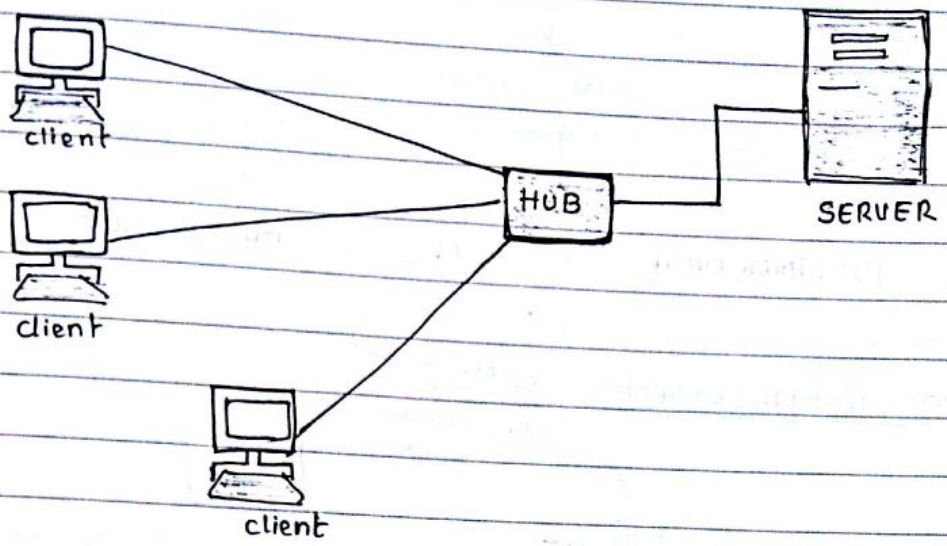
TELECOMMUNICATION AND NETWORKS

[PART 2/2]

– Syam Reddy
7207000086

Q33: client/server Architecture:



* In this model/server, number of computers, known as clients are connected to a single host computer known as server.

* It uses a dedicated server which provides various services to clients like hardware, software and data access.

* clients can share disk storage and printers attached with the server.

* Data transfer speed is more

* It is suitable for large organisations having large no. of clients.

* clients are required to be connected with server in a particular structure [star, Bus, Mesh etc...)

* This architecture is Employed when data security is of prime importance.

* The components of c/s model are
  (i) client
  (ii) server.

★ " client is a process (normally running on a workstation (or) pc) running the front end part applications "

(a) clients

client's can also be known as workstations

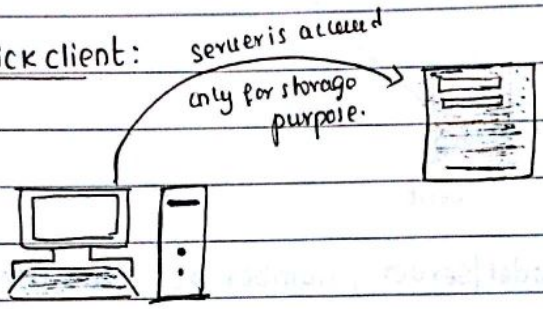
↓

Three types of clients

↓ ↓ ↓

Fat / Thick client | Thin client | Hybrid client

1. FAT client | Thick client:



3 A fat client is a client that performs the bulk of any data processing operations itself and does not rely on the server.

3 unlike the thin clients, Thick clients doesnot rely on the central processing server because the processing is done locally on the user system, and the server is accessed primarily for storage purposes.

3 However, use of fat client is not well suited for distributed applications Bcos Any software (or) processing upgrade will need to be implemented in all the clients

whereas if all the processing is maintained at server than upgrade will be need at server only.

Example: personal computers.

2. Thin client:

- This type of client doesnot maintain processing part of application
- It maintains only interface for inputs and outputs
- A thin clint generally present only processed data prouided by an application server.
- A deuice using web application is a thin client.

3. Hybrid client:

A Hybrid client is a mixture of the Thick and Thin client models.

- similar to a fat client, it process locally,

But

Relies on the server for storing persistent data.

↓

Hybrid clients are well suited for videogaming.

Q.33(i) Working of a client/server architecture:

The following describes the working of a client/server Network:

- client/server technology consists of a client process and server process.
- client process and server process can be on same computer (or) separate computer.
- client (or) server system can be upgraded independently.
- The server can provide service to multiple clients and in some cases client can access multiple servers.
- some portion of processing application may reside on a client
- Action is usually initiated at the client end, not at the server End.
- The Network system implemented within the client/server technology is commonly called by the computer industry as Middleware.

  Middleware is all the distributed software needed to allow client and servers to interact.

- Middleware allows for communication, directory service, queuing, distributed file sharing and printing.

Q33(iii) Characteristics and issues of client/server Architecture:

Characteristics:

☺ Services

c/s technology is Based on the concept of service delivery. In this

server is a service provider and

client is a service consumer.

☺ Shared Resources:

A server provides service to many clients simultaneously and regulate their access to shared resources.

☺ Transparency of location:

c/s software usually masks the location of the server from the clients.

ie.., generally, client is not aware of server location.

☺ Mix and Match:

c/s software is generally* independent of Hardware and operating system used in the Network.

☺ Scalability:

c/s allows to connect and disconnect the client without affecting performance.

☺ Integrity:

Data is centrally managed in server and Thus help (or) provide better management of database and data upgradation etc..., & Helps to provide better data integrity.

issues:

☹ single point failure:

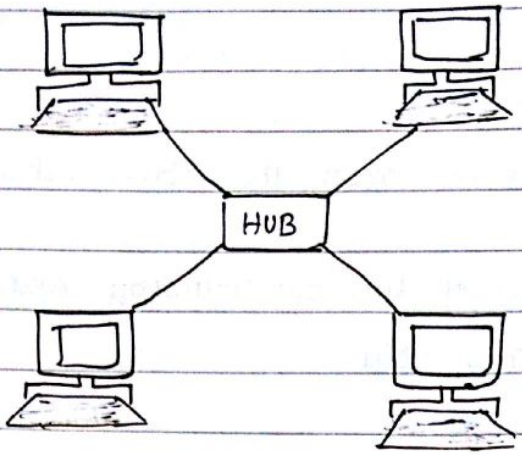
if server is down, the entire network stops working.

☹ simultaneous access of data and services by many users may result in slow processing of data.

☹ complexity:

Managing distributed system is complex task.

Q34: PEER-TO-PEER Networking:



- In this architecture,
  No dedicated servers are used
  "All computers are at Equal levels, And therefore termed as PEERS"

- Normally, Each computer can function Both as client and Server.

- This type of arrangment is suitable when limited no. of users are there and security of data is not a very important criteria.

- The main advantage of this architecture is simplicity of its design and maintenance.

- A P2P network can be an adhoc connection
  ie.., a couple of computer connected via a universal Serial bus to transfer files.

☞ The primary goal of a P2P file sharing Network, is that many computer come together and pool their resources to form a content distribution system.

Advantages:

(i) peer-to-peer Networks are easy and simple to set-up.

(ii) It is very simple and cost effective

(iii) if one computer fails, it will not effect the working of other connected computers.

Disadvantages:

☹ The data security is very poor in this architecure.

☹ It is not useful network model if large number of computers are required to be connected.

☹ Data sharing/accessing files is problematic, if computers are not connected properly.

Q35: Multi - Tier Architecture:

⁂. Tier ⟶ Distinct part of Hardware (or) Software.

[Here TIER stands for how network application is divided into different processes which can work independently]

⁂. Single - tire System / one - tier system / Architecture :

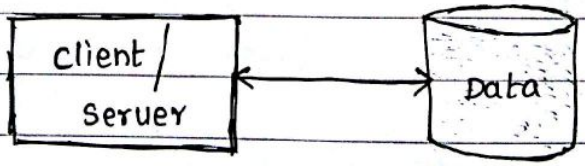
☞ If all the components of network application are required to be placed on a single server (or) single platform Then it is known as single tire architecture.

[ie .., A single computer that contains a database and a front - end (GUI) to access the database is known as single - Tier system]

☞ In This There is No separation b/w Server and client ie .., Both are integrated together.

☞ Generally,
This type of Business system is used in small Businesses.

☞



Advantages:

- A single-tier system requires only one stand-alone computer.
- It also requires only one installation of proprietary software which makes it the most-cost effective system available.

Disadvantages:

- It can be used by only one user at a time.
- Single-tier application are impractical when multiple users want to use the same application, simultaneously.

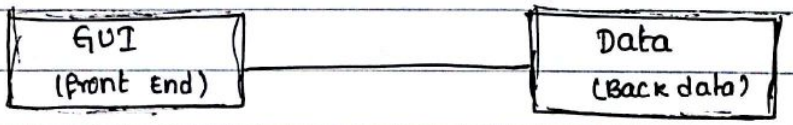
※. Two-tier system | Two-tier Architecture:

☞ Two-tier architecture is traditional client/server system which divides the application into two parts.

one is client & second is server.

client provides interface for access of services and server provides the service.

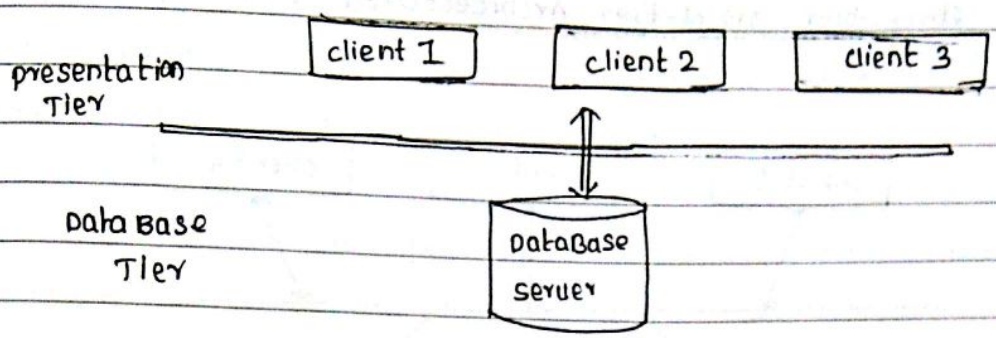
→ Generally, these two portions are known as Front End and Back End.



→ Here GUI is an interface known as Graphical user interface is also refered as presentation layer.

☞ A two-tier Architecure is a software architecure in which a presentation layer (or) interface runs on a client, and

A data layer (or) data structure gets stored on a server.



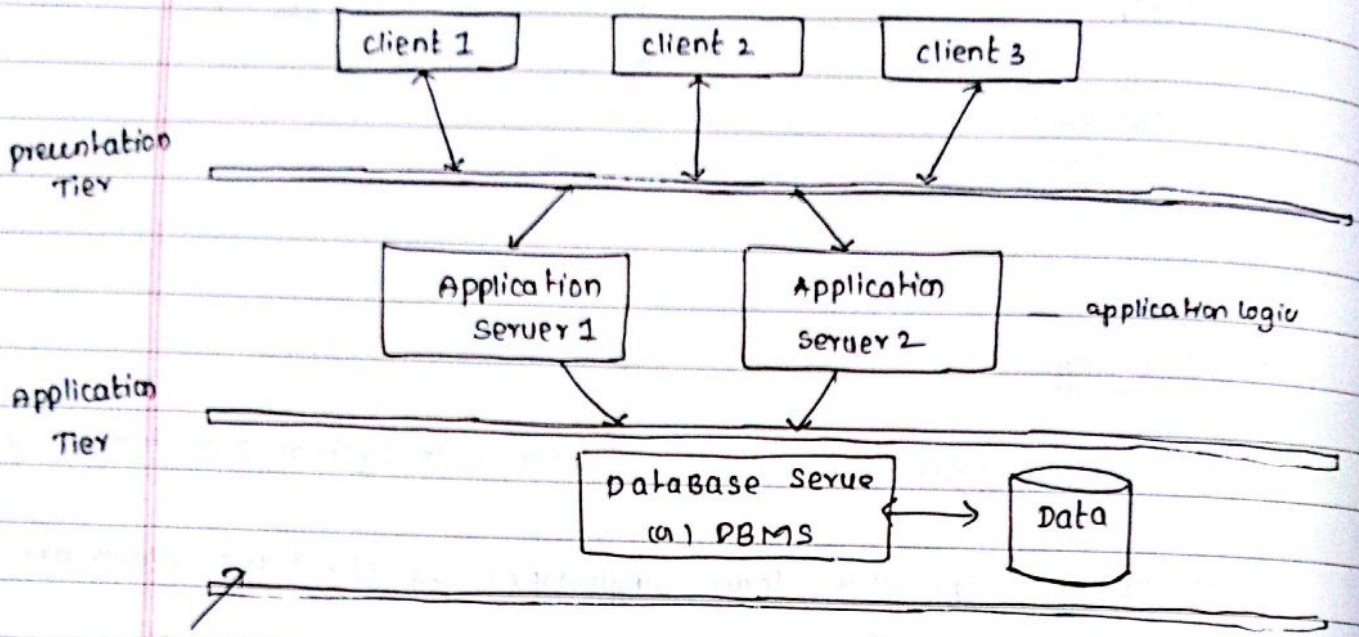
Aduantages:

- Multiple users can access ~~internet~~ with system simultaneously.
- Better performance than single tier as client and server are separate process.
- simple to setup and maintain.

Disaduantages:

- cannot support large no.of users as performance starts decreasing if no.of users increases.
- Less flexible

※ Three-tier (or) N-tier Architecture:

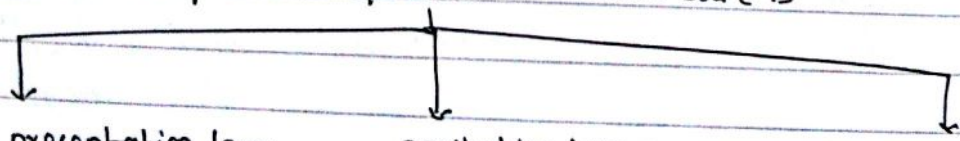


☞ In Three-tier architecture,

The application components are divided into 3 logical categories (or) parts.

Now a days, most widely accepted form of c/s model is Based on 3-tier architecture.

☞ The components of 3-tier architecture is



The presentation layer	Application layer	DataBase server
[used for input and output data/information]	[used for processing data]	[it maintains data & provides data mgt. services]

* The three tier architecure is used when an effective distributed cls design is that provide increased performance, flexibility, maintainability, reusability and scalability.

* The place where the application logics are maintained in the three-tier architecture is known as middleware.

Advantages:

☺ clear separation of user-interface-control and data presentation from application-logic
[with this separation more clients are able to have access to a wide variety of server applications]

☺ Dynamic Load Balancing:
in case of performance bottleneck during peak hours the load can shifted to other services servers in n-tier architecture.

☺ Easy to change and manage complex distributed applications such as Banking and telecom application.

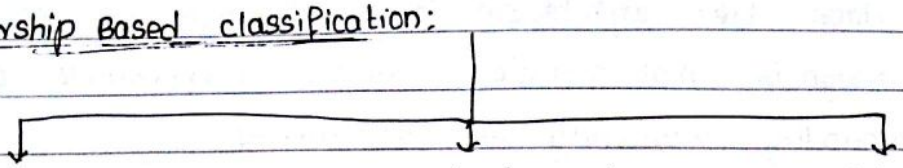
Disadvantages:

☹ Require high technical expertise to manage this architecture

☹ Managing Network traffic, fault tolerance and load Balancing in real-time require complex and costly tools.

☹ More suitable for distributed applications.

Q36: Ownership Based classification:



Q.36(i) public Network:

- public data Network is a network shared and accessed by all users across the world.
- It is a Network established and operated by a telecommunications, administration for the specified purpose of providing data transmission service for the public.

Ex: Internet.

- public data Network provide, low cost services as setup costs are shared among large number of organization and users.

However,

Data security risks higher in the public data network Than private data Network.

Q36(ii) **private data Network:**

private Network is used by particular organization, particular campus (or) particular Enterprise only.

→ This is a network that is not available to the outside world.

Ex: Intranet.

Q36(iii) **Virtual private Network:**

⁂ VPN is a Network which helps users to connect to their private Network (intranet) from any location using public Network (internet)

⁂ virtual means not actual;
Therefore VPN is not a pre-established Network.
it is a Network, which users established on need basis from anywhere using internet.

⁂ In VPN, a software known as VPN client or dialer is used which provides access to authorized users for their private Network from any location just like a user get access to its Network from its actual place.

⁂ VPN has became a popular Network concept to provide Network accessibility to organization's Employees from anywhere.

Q37: Network Risks, controls and Security:

※ Network security:

Network security consists of provisions made in an underlying computer Network infrastructure, policies adopted by the Network administrator to protect the Network and the Network accessible resources from unauthorized access.

※ Need for security:

The Basic objective of prouiding Network security is to

- Safe guard assets
- Ensure and maintain data integrity.

※ Types of Security:

- **physical Security** → it is implemented to protect physical assets like CD, Harddisk etc..,
- **Logical Security** → It is implemented to protect logical assets like data, programs etc..,

Q37(1) Possible Threats and vulenarabilities involved in system security.

Threats:

Threat is anything which can cause Economic and Reputation losses due to

- Disruption in operation
- Error in system
- Data security issue.

There are different types of threats to Network systems, For Example. fire damage
water damage
voltage fluctuations
disaster
intrusion (unauthorised accen)
viruses
misuse of hardware & software,
hacking of data etc..,

⇒ Threats can be broadly categorised as

- unstructured threats
- structured threats
- External threats
- internal threats.

(i) unstructured threats:

- These orginates mostly by inexperienced individual's, out of curosity and new learning by using easily available hacking tools from the internet.
- Most of them are done out of curosity/interest rather than with a maticious intention

Ex: use of External disk in the organization computer without proper scanning.

(ii) structured threats:

- These are intentional threats and originate from persons who intentionally want to damage the organization system
- Generally they target specific destination (or) group.
- usually,
  These hackers are hired by organized crime, industry competitors etc.,

(iii) External threats:

These orginate from individuals who donot work with organizations but does have authorized access to organization system (or) Access the system without authorization;

(iv) internal threats:

Typically,

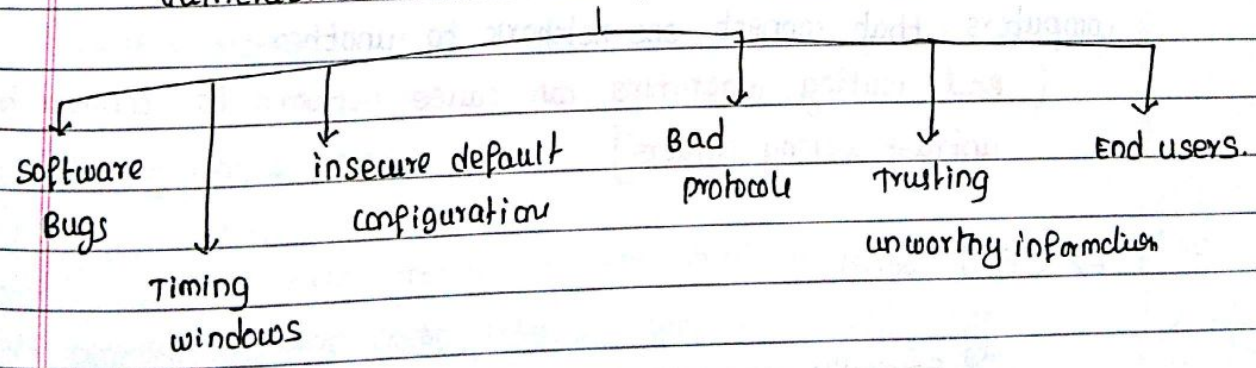
These threats are primarily from the Employees of organization [ie.., who have authorized access to the Network]

⁂ Vulnerabilities:

Vulnerability is an inherent weakness in the
design
configuration (or)
implementation of a network (or) system
that renders it susceptible to a threat.

↓

∴ The following factors are responsible for occurrence of vulnerabilities in the software:



a] Software Bugs:

Software bugs (or) Errors are quite common and Expose the system for different threats (or) risks.

[Bug (or) Error in software is a serious vulnerability]

b] Timing windows:

↳ This problem may occur when a temporary file is Exploited by an intruder to gain access to the file, overwrite important data and use the same file as a gateway for advancing further into the system.

c] insecure default configuration:

using well known and easily guessed passwords can cause vulnerability.

d] Bad protocols:

using inefficient non-standard protocals, by which information is exchanged over the internet may cause vulnerability.

e] Trusting untrustworthy information:

↳ This is usually a problem that affects routers (or) those computers that connect one network to another.

[Bad routing algorithms can cause network to connect to untrust worthy servers]

f) End users:

↳ Generally, users of computer system are not professionals and are not always security conscious.

Q3.3(ii) Short Notes on Network Security:

☞ Network security is a provision made to protect the network from threats.

⇓

The Network security involves 4 aspects:

i] privacy:

→ privacy means that the sender and the receiver expect confidentiality.

→ The transmitted message should make sense to only the intended receiver and the message should be unintelligible to unauthorized users.

→ This is achieved by cryptography and Encryption techniques.

ii] Authentication:

preventing unauthorized user from accessing Network data.

iii] integrity:

This means that the data must arrive at the receiver exactly as it was sent.

↳ There must b not be any changes during the transmission - [either accidentally (or) malicious]

iv] Non-Repudiation:

This means that a receiver must be able to prove that a received message came from a specific sender and the sender must not be able to deny sending it.

Q38 NETWORK SECURITY PROTOCOLS:

Network security protocols are primarily designed to prevent any unauthorized user,
application,
service (or)
device from accessing Network data.

↳ it includes using cryptography and its algorithms for data Encryption and decryption.

a] what is cryptography:

cryptography is a science (or) study of techniques and practices used for secure data communication in presence of third parties.

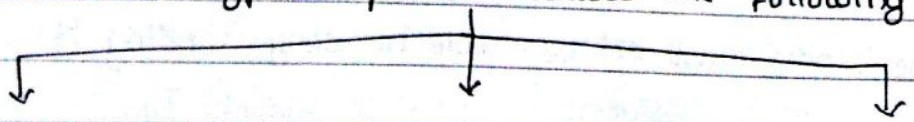
↳ it is use of protocols and algorithms to Ensure data confidentiality, integrity and authentications.

[ie.., it transform data into codes that appear meaningless to any one whodoesnot have authentication to access the respective data/file]

b] Encryption:

Encryption is the process of Encoding messages (or information) in such a way that hackers (or) eavesdroppers cannot read it
ie..,
only authorised users can read the message.

→ The Encryption process includes the following components



a] plain text:

It is the message that is to be Encrypted.

b] cipher text:

It is the output of the Encryption process that is to be transmitted.

c] Encryption model:

This includes different aspects related to Encryption & decryption of message.

For Example: Encryption and decryption keys and Encryption algorithams.

⇓

intruder

Actiue intruder

⇓

These type of intruder can not only listen to the communication channel, But also record messages & play them back (or) modify messages before they reach to the receiuer.

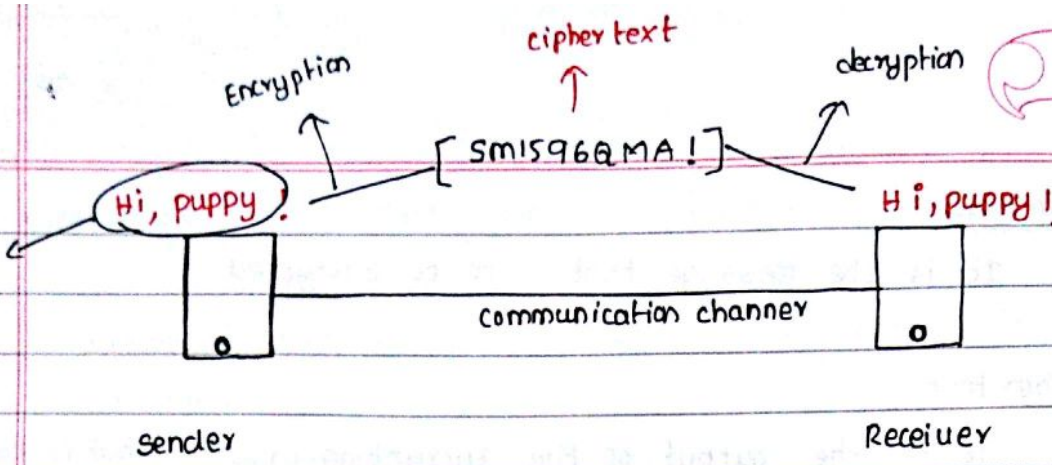
passiue intruder

⇓

These type of intruder will only listen to the communical channel

⇓

However, unlike the intended recipient, he doesnot know what the decryption key is and so cannot decrypt the cipher text easily.



※ The art of Braking ciphers, known as cryptanalysis, and the art of devising them (cryptography) are collectively known as cryptology.

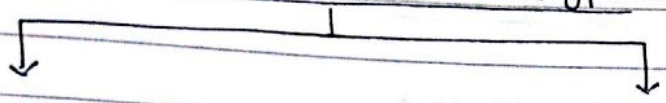
c] There are two categories of Encryption | decryption methods:

- Secrete key method
  (in this the same key is used by Both sender and receiver)
  - The sender uses this key and an encryption algoritham to encrypt data; and
  - The receiver uses the same key and decryption algoritham to decrypt the data
- public key method
  in this method there are two keys
  - public key ⇓ This public key is announced to public by sender
  - private key ⇓ The private key is kept by the receiver.

In this,

The algorithm used for decryption is the inverse of the algoritham used for Encryption.

d] There are two approaches for Encryption:



Hardware Encryption

Software Encryption.

i] Hardware Encryption:

These devices are programmed to transmit data in an encrypted form and decrypt the received encrypted data.

☞ These devices are used among Branch offices for transfer of information in a secured manner.

☞ Hardware Encryption devices are available at a reasonable cost, and can support high-speed traffic.

ii] Software Encryption:

In this, Encryption is performed using some software applications

☞ This is more popular than hardware encryption as this allows a secured data communication b/w different organisations

for Example:

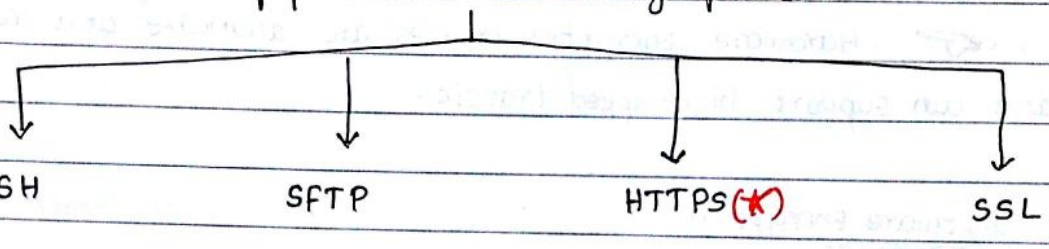
when a user communicates with Bank during net Banking it is software Encryption [ie.., providing Encryption & decryption for message security]

38(ii) popular Network security protocols:

as we know from Q:38 that

"Network security protocols are primarily designed to prevent any unauthorised user
application
device (or)
service from accessing Network data.

- some of the popular Network security protocols include



a] SSH : [secure shell]

Secure shell is a program to log into other computer over a network, to execute commands in a remote machine, and to move files from one computer to another.

☞ secure shell provides strong authentication and secure communication over insecure channels.

☞ SSH protects Network from attacks such as IP spoofing, IP source routing, DNS (Domain name space) spoofing,

- once SSH encryption is enabled an attacker cannot access the system because all the data communication b/w remote user & system is occurs in Encrypted form.

b] SFTP :

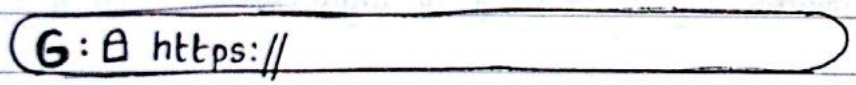
it is known as SSH file transfer protocol [or] Secured file transfer protocol.

☞ SFTP encrypts both commands and data, preventing, passwords and sensitive information from being transmitted in telecommunication network.

imp c] HTTPS: [HYPERTEXT Transfer protocol secure]

it is a communication protocol used for secure communication of web pages b/w user and web server.

☞ in this, data is transmitted in encrypted form by using public key and then this can be decrypted by the web server only, thus no one in between can read the information.



d] SSL: [secured socket layer]

It provides a secured channel between two machines operating over the internet (or) internal network.

☞ It is an extension of HTTPS

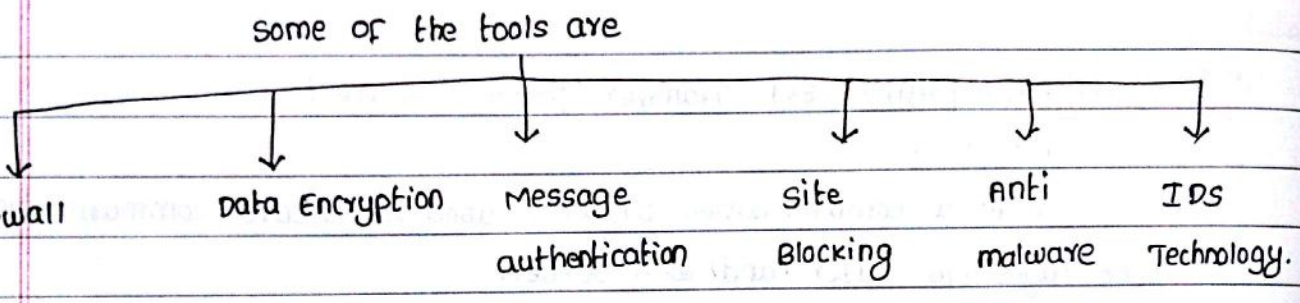
☞ It is used b/w Browser and web server.

[It is mainly used for net Banking transactions & online payment]

※ The main difference b/w HTTPS and SSL is that encryption is stronger in the SSL (or) Bits used in the key for encryption are higher in SSL than used in HTTPS.

38(iii) Explain various Network security techniques [or]
what tools are available to protect the information in Network against intrusion (or) misuse?

Ans: several tools are available to protect information (=data) & systems from unauthorised intrusion, misuse and viruses etc..,

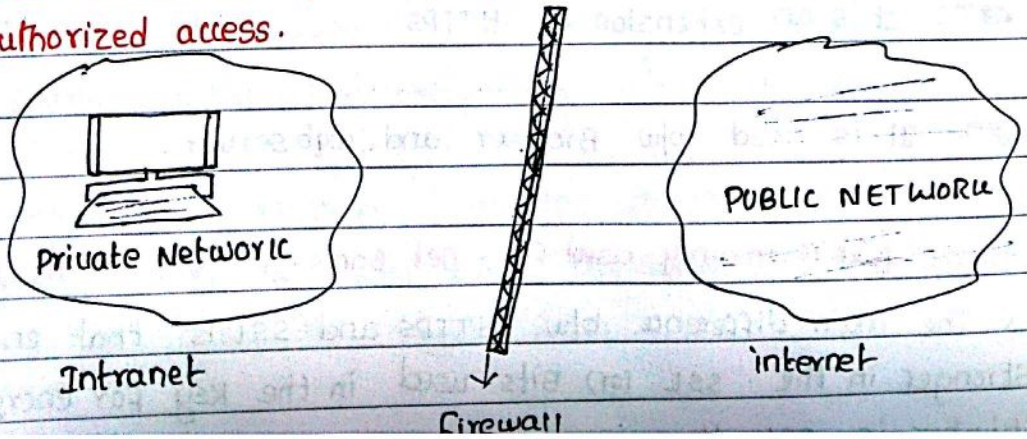


a] Firewall:

Firewall is one of the most popular techniques of Network security. Firewall provides Logical security to organization data & Network.

☞ it forms a Barrier [Fence] between a secure and an open Network/Environment

↳ Firewall is a computerized Electronic system (mainly Firewalls are specialized softwares), installed b/w organization private Network & public Network to protect organization private Network from unauthorized access.



* Firewall acts as insulator which insulate organization private Network from invaders coming through public Network.

b] Data Encryption:

[see pg:83]

c] Message authentication:

It makes sure that a message is really from whom it is supposed to be.

[and]

is not tampered in between.

d] Site Blocking:

This software helps in blocking site that are deemed inappropriate by management, for visit/access by Employees.

[proxy server is used for site blocking]

e] Anti-malware:

Anti malware Network tools helps administrators to identify, Block and remove malware.

f] IDS [intrusion Detection system] technologies:

[will be discussed as separate topic in Next pg: ie 91]

3S(iv) IDS: [intrusion Detection system]

↳

The Goal of intrusion detection system is to

- monitor the Network assets
- & detect anomalous behaviours & misuse.

* though there are several measures which help to prevent unauthorized entry into the system such as userid-password, firewall etc..,

But the fact is even though with all these security measures are in place there can be some sort of unauthorized activities on enterprise Network.

↳ Therefore,

"specific intrusion detection measures are required to detect such unauthorized activities"

⇓

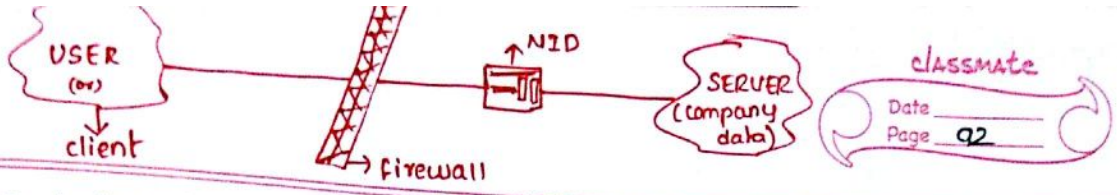
There are 4 popular IDS Technologies

- NID
- HID
- NNID
- Hybrid intrusion Detection.

a] Network intrusion detection: [NID]

In this, a special device is placed in the Network system, nearby the server [in the communication link] in search of unwanted [or] malicious events on the wire b/w Hosts.

* ☞ Typically referred to as "packet-sniffers"

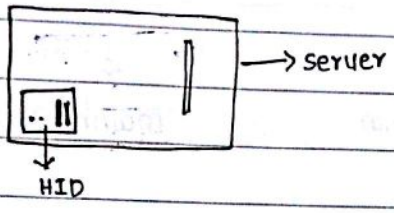


☞ NID device intercept packets travelling in different communication channels.

↳ once captured the packets are analyzed in a number of different ways.

☞ NID is designed especially to monitor & detect threats from external users.

b] Host - Based intrusion detection [HID]



This type of system is actually installed in the server [host] (or) system being monitored.

☞ HID is designed especially to monitor & detect threats from internal users [internal threats]

☞ The difference b/w HID and NID is that NID deals with data transmission from Host to Host while HID is concerned with what occurs on the Host(server) itself.

c] Network Node intrusion detection(NNID)

↳ This is an extention of NID, with NNID the packet sniffer is positioned in such a way that it captures packets after they reach their final target [ie., the destination host], Then the packet is analysied.

d] Hybrid intrusion detection:

↳ This IDS offers features of Both NID and HID devices.

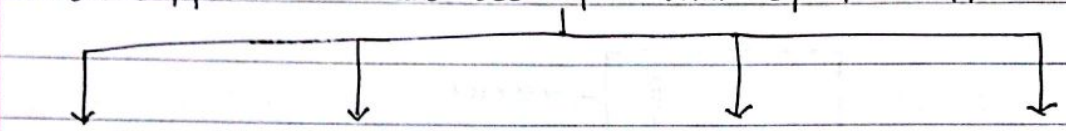
☞ This provide the logical complement to NID & HID

ie.., central intrusion detection management for Both internal & external threats.

Q: 39 Network administration and Management:

(Not much important ; so we are not going to discuss in detail manner)
Just covering headings)

Network management and administration refers to the activities, methods, procedures and techniques that help for efficient

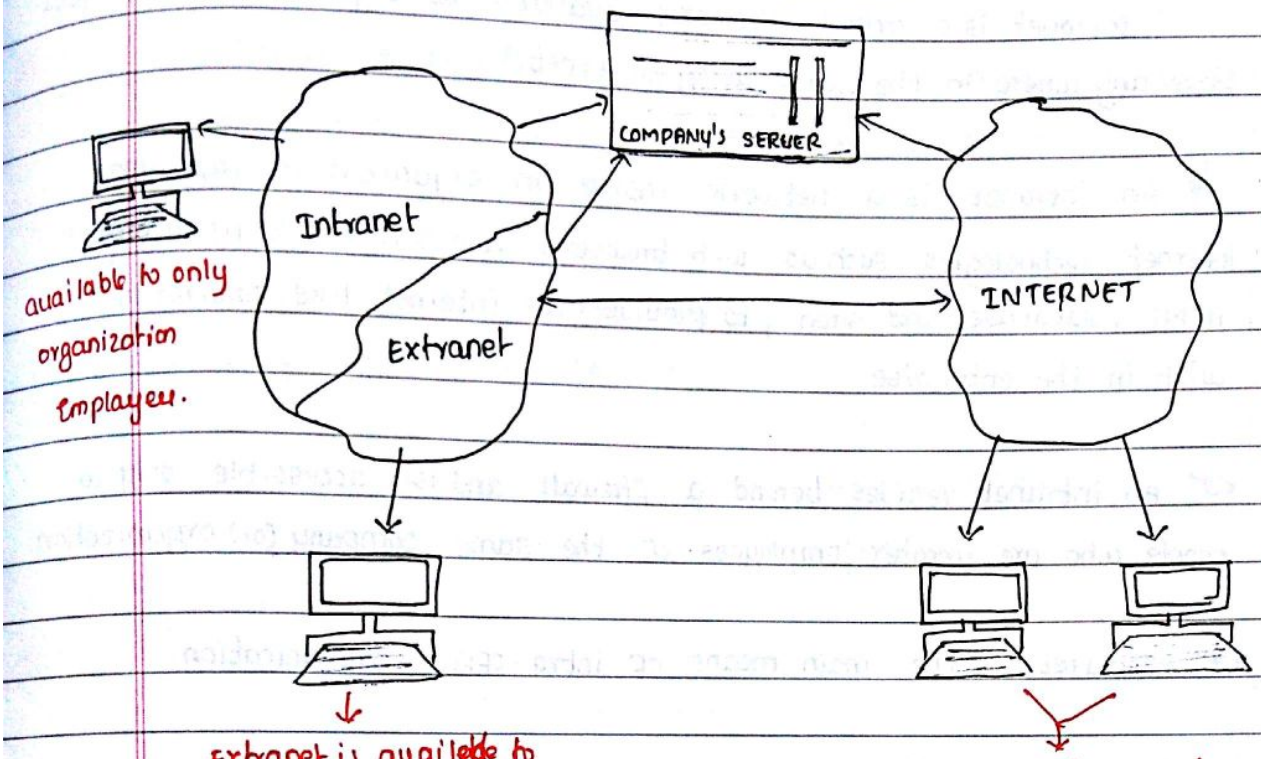


operation administration maintenance & provisioning of Network systems.

※ There is a common term to characterize the Network management functions known as FCAPS

* F ⇒ Fault management
* C ⇒ configuration management
* A ⇒ Accounting Management
* P ⇒ performance Management
* S ⇒ Security management.

Q: 40 Short Notes on intranet, Extranet and internet:



a] Internet:

.⁘. The internet is a massive global system that connects computer Networks around the world together.

.⁘. The internet uses the standard internet protocol suite (TCP/IP) to allow us to connect to Each other.

.⁘. it has various information resources & services, such as The web pages of world wide web(WWW), Games, Videos, images, email etc..,

.⁘. It also Enables New forms of human interaction through, instant messaging, E-mail, internet forums, & social Networking.

b] Intranet:

"Intranet is a private Network available to organization Employees from any where in the world using internet."

↳ An intranet is a network inside an organization that uses internet technologies such as web browsers and servers, TCP/IP protocols, HTML, database and soon, to provide an internet like Environment with in the enterprise.

☞ An intranet resides behind a firewall and is accessible only to people who are members/Employees of the same company (or) organization.

☞ Intranet is the main means of intra-office communication.

☞ An intranet is protected by security measures such as passwords, Encryption, and firewalls, and thus can be accessed by authorized users through the internet.

Advantages:

- Easier and faster Access to information
- collaborative, group working is possible.
- much less expensive to Build & manage.
- Easy and fast to share resources/data/information.
- can share Hardware devices (such as printer/scanner/fax etc)

c] Extranet:

Extranet is an extension of intranet, which makes organization intranet to be accesible to outsiders like Business associates (like suppliers, vendors, partners & customers etc..,)

·※· people from outside the company can have a limited access to the company's internal network for

- Business (or)
- education related purpose.

in simply put,

Extranet refers to an intranet that is partially accessible to authorized outsiders.

[or]

it is the company's website for its customers and vendors.

Application of

internet

* Low cost communication
* Hub of information [ie., Knowledge Base]
* E-commerce
* Social Networking/chat rooms
* software & data files download
* Data publishing

intranet

* workgroup communications
* sharing of resources
* sharing of devices
* collaborative working

Extranet

* Exchange large volume of data with Each other using EDI [Electronic data interchange]
* share news of common interest exclusively with partner companies.
* To share product catalogues with wholesaler (or) dealers in trade.

J.UU gmp

Q40: E-COMMERCE:

- E-commerce is the process of doing Business electronically. (ie on-line)
- E-commerce started with the inuention of Electronic data interchange [E.D.I]
- it inuolues automation of variety of Business-to-Business and Business-to-customer transactions through reliable & secure connections.
- E-commerce is not a single technology but a combination of sophisticated technologies and Business services integrated to prouide instant transaction & response to customer.

  [For Example, e-commerce is collection of internet, intranet, mail, fax, EDI etc to prouide online commerce service]

- E-commerce is associated with buying and selling of information, products & services via computer networks.

Q.no(ii) Risks involved in E-commerce:

The risks associated with e-commerce are versatile.

↳ some of the risks associated with e-commerce are

a] problem of anonymity:

There is a need to identify and authenticate users in the virtual global market [where any one can sell/buy, anything from anywhere.

b] Repudiation of contract:

There is a possibility that the electronic transaction in the form of contract, sale order (or) purchase by the trading partner (or) customer may be denied.

c] Lack of authentication of transactions:

The electronic documents that are produced in the course of an e-commerce transaction may not be authentic and reliable.

d] Data loss (or) theft (or) duplication:

The data transmitted over the internet may be lost, duplicated, tampered (or) replaced.

e] Attack from hackers:

Hacking of important data and information.

f] Denial of service:

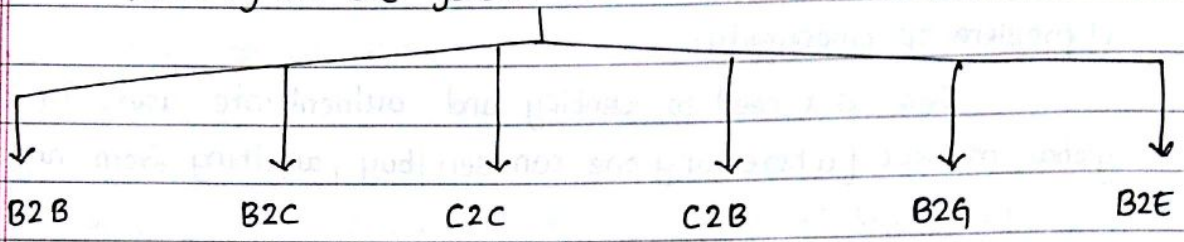
Service to customers may be denied due to non-availability of system as it may be affected by viruses

g] Lack of audit trails

Q.no(iii) Different types of E-commerce (or) Different classes of E-commerce:

E-commerce is associated with buying and selling of information, products & services via computer Networks.

↳ Following are the general classes of e-commerce applications.



a] Business-to-Business (B2B) e-commerce:

☞ B2B refers to the exchange of information, services and/or products from one Business to another.

Ex: i) Tvs company selling its tyres to Leading Bike manufacturer Heromoto corp Ltd online using B2B e-commerce

ii) Hy intel is selling its chips to computer manufacturer online using B2B.

b] Business-to-customer (B2C) e-commerce:

☞ It is defined as exchange of resources, services, information and/or products from a Business to a customer.

Example:

Two types

- Social sites — www.tisco.com
- Transactional sites — www.amazon.com

* Social sites are informative sites, these sites provide only information on products & services offered by various organizations to its customers

* The transactional sites are those e-commerce sites which allow conducting transactions of sale & purchase.

c] customer to customer [C2C]: [or] consumer to consumer

☞ C2C e-commerce is an internet-facilitated form of commerce that provides a virtual Environment in which consumers can sell to one another through a third party intermediary.

Ex: olx
QUIKER

d] consumer to Business [C2B]:

☞ In C2B e-commerce model

" consumers directly contact with Business vendors by posting their project work online so that the needy companies review it and contact the consumer directly with Bid.

Ex: freelancer.com

e] Business to Government [B2G]

☞ B2G e-commerce is also known as E-Governance

↳ in which use of information and communication technologies to Build and strengthen relationships b/w Government & Employees, citizens, NGO, & Business etc..,

Ex: e-Governance [IRCTC]

F] Business-to-Employee [B2E]:

☞ B2E e-commerce, from an intra-organizational perspective, has provided the means for a Business to offer online products & services to its Employees.

Q.41 MOBILE COMMERCE: [M-commerce]

- M-commerce is an extended form of e-commerce.
  - In this technique, Business services are provided through internet Enabled mobile phones and personal digital Assistance (PDA).
- M-commerce is the Buying and selling of goods and services through wireless handheld devices such as mobile phone and PDA's etc..,
- The m-commerce is known as next generation e-commerce.
- The technology Behind m-commerce is WAP [wireless application protocol]
- The content delivery over wireless devices are faster, more secure and scalable.

So, there is a speculation that m-commerce will surpass (=overcome) wireline e-commerce.

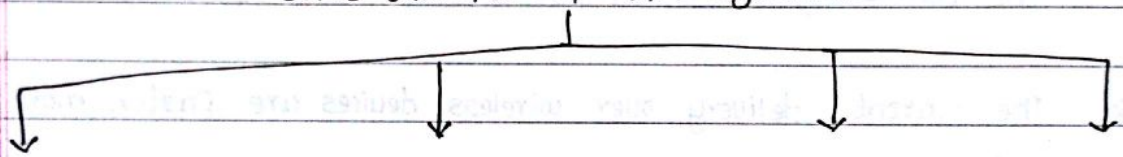
Q42: ELECTRONIC FUND TRANSFER: [EFT]

☞ EFT represents the transfer of funds into a person's Bank account, electronically.

☞ EFT is faster and safer money transfers method; and money is transferred immediately into an account by using online banking solutions in-place of cheques and drafts

⁂ The payment mechanism moves money between accounts in a fast, paperless way.

SOME EXAMPLES OF EFT SYSTEMS



ATM's [Automated Teller machines] | POS [point of sale transactions] | Preauthorized transfer | Telephone transfer

ATM's:

Now widely used Everywhere by Banks

⁂ consumer can do their Banking without the assistance of a Teller.

⁂ consumers can Now get cash, deposit cash, transfer funds, pay bills by using ATM's.

POS:

This allows the use of credit (or) debit cards [EFT cards] to allow transfer of funds from consumer Bank account to merchant account, directly.

preauthorized transfer:

This is a method, which provides depositing (or) withdrawal of funds from an individual account, when an account holder authorizes the Bank to do so.

↳ For Example:

The consumers can authorize their Banks to direct Electronic deposit/transfer of wages, Bills & dividends from their accounts etc..,

Telephone transfer:

consumers can transfer funds from one account to another through telephone instructions rather than traditional written authorisation.

Ex: you can order payment of specific bills by phone.