Chameli Devi Group of Institutions, Indore
Department of ESH
BT205 Basic Computer Engineering
B. Tech, CSE and IT (II Semester)
Unit -4

……

Computer Networking: Introduction, Goals, ISO-OSI Model, Functions of Different Layers. Internetworking Concepts, Devices, TCP/IP Model. Introduction to Internet, World Wide Web, E-commerce

Computer Security Basics: Introduction to viruses, worms, malware, Trojans, Spyware and Anti-Spyware Software, Different types of attacks like Money Laundering, Information Theft, Cyber Pornography, Email spoofing, Denial of Service (DoS), Cyber Stalking, Logic bombs, Hacking Spamming, Cyber Defamation, pharming Security measures Firewall, Computer Ethics & Good Practices, Introduction of Cyber Laws about Internet Fraud, Good Computer Security Habits.

Unit Objective: To familiarize the students with basic concepts of computer networking and security basics.

Unit Outcome: Student should be able to explain the networking and security concept with their practical applications in the real world.

……..

Computer Network

A computer network is a set of devices connected through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels. Computer Network is a group of computers connected with each other through wires, optical fibers or optical links so that various devices can interact with each other through a network. The aim of the computer network is the sharing of resources among various devices.

Uses of Computer Network

Resource sharing: Resource sharing is the sharing of resources such as programs, printers, and data among the users on the network without the requirement of the physical location of the resource and user.

Server-Client model: Computer networking is used in the server-client model. A server is a central computer used to store the information and maintained by the system administrator. Clients are the machines used to access the information stored in the server remotely.

Communication medium: Computer network behaves as a communication medium among the users. For example, a company contains more than one computer has an email system which the employees use for daily communication.

E-commerce: Computer network is also important in businesses. We can do the business over the internet. For example, amazon.com is doing their business over the internet, i.e., they are doing their business over the internet.

Types of Computer Network

LAN: Local Area Network is a group of computers connected to each other in a small area such as building, office. LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc. It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables. The data is transferred at an extremely faster rate in Local Area

Network. Local Area Network provides higher security.

PAN: Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters. Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network. Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

MAN: A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network. Government agencies use MAN to connect to the citizens and private industries. In MAN, various LANs are connected to each other through a telephone exchange line. It has a higher range than Local Area Network (LAN).

WAN: A Wide Area Network is a network that extends over a large geographical area such as states or countries. A Wide Area Network is quite bigger network than the LAN. A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links. The internet is one of the biggest WAN in the world. A Wide Area Network is widely used in the field of Business, government, and education.

Network Topology

Topology defines the structure of the network of how all the components are interconnected to each other. The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as Network Topology.

Bus Topology: The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable. Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable. When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not. The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks. The configuration of a bus topology is quite simpler as compared to other topologies.

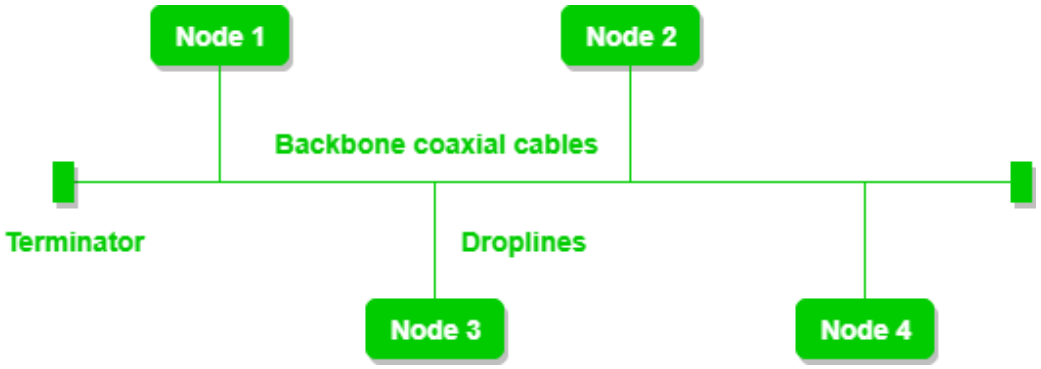

Figure 4.1: Bus Topology

Ring Topology: Ring topology is like a bus topology, but with connected ends. The node that receives the message from the previous computer will retransmit to the next node. The data flows in one direction, i.e., it is unidirectional. The data flows in a single loop continuously known as an endless loop. It has no terminated ends, i.e., each node is connected to other node and having no termination point. The data in a

ring topology flow in a clockwise direction.

Figure 4.2: Ring Topology

Star Topology: Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer. The central computer is known as a server, and the peripheral devices attached to the server are known as clients. Coaxial cable or RJ-45 cables are used to connect the computers. Hubs or Switches are mainly used as connection devices in a physical star topology. Star topology is the most popular topology in network implementation.

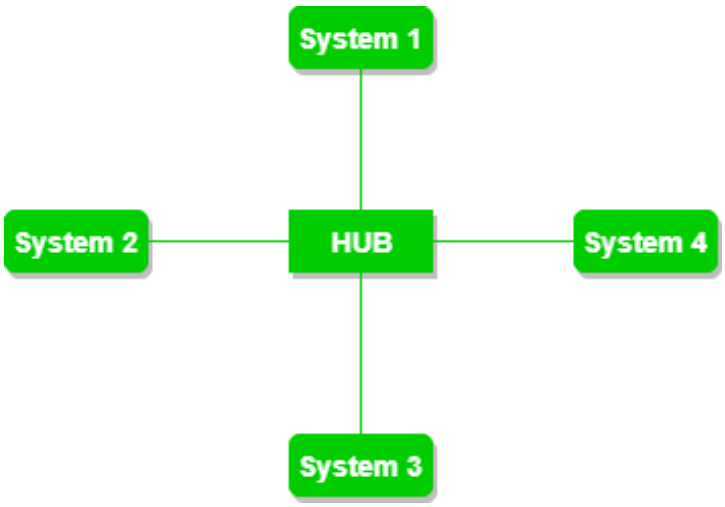

Figure 4.3: Star Topology

Tree Topology: Tree topology combines the characteristics of bus topology and star topology. A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion. The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node. There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

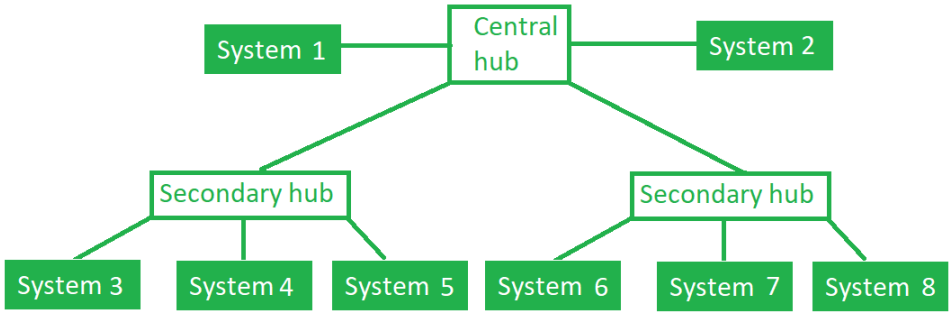

Figure 4.4: Tree Topology

Mesh Topology: Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections. There are multiple paths from one computer to another computer. It does not contain the switch, hub or any central computer which acts as a central point of communication. The Internet is an example of the mesh topology & mainly used for wireless networks. Mesh topology is mainly used for WAN implementations where communication failures are a critical concern.

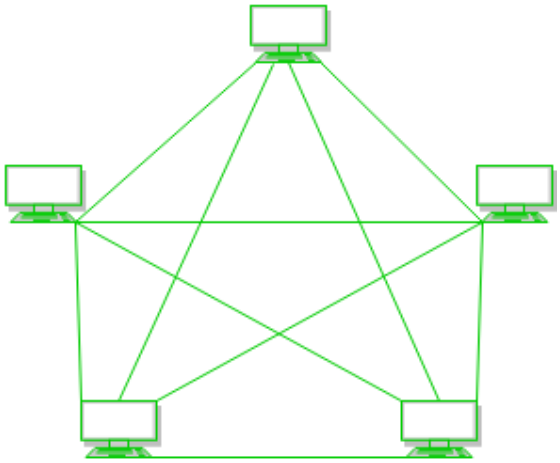

Figure 4.5: Mesh Topology

Hybrid Topology: The combination of various different topologies is known as Hybrid topology. A Hybrid topology is a connection between different links and nodes to transfer the data. When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology.

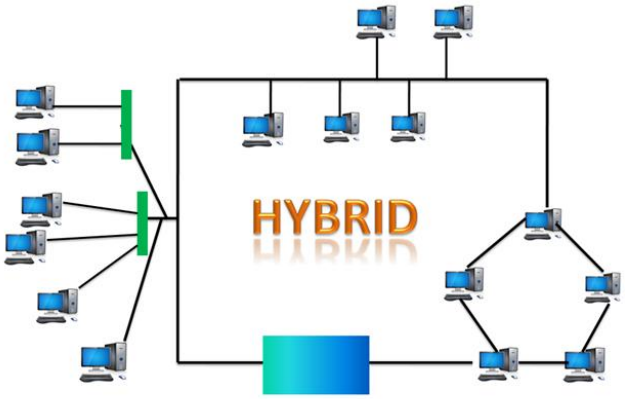

Figure 4.6: Hybrid Topology

Networking Devices

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another.

Following are the networking devices:

- Repeater
- Hub
- Bridge
- Switch

- Routers
- Gateway
- NIC

Repeater: A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

Hub: A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Bridge: A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2-port device.

Switch: A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

Router: A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

Gateway: A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

NIC: NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and the router or modem. NIC card is a layer 2 device which means that it works on both the physical and data link layers of the network model.

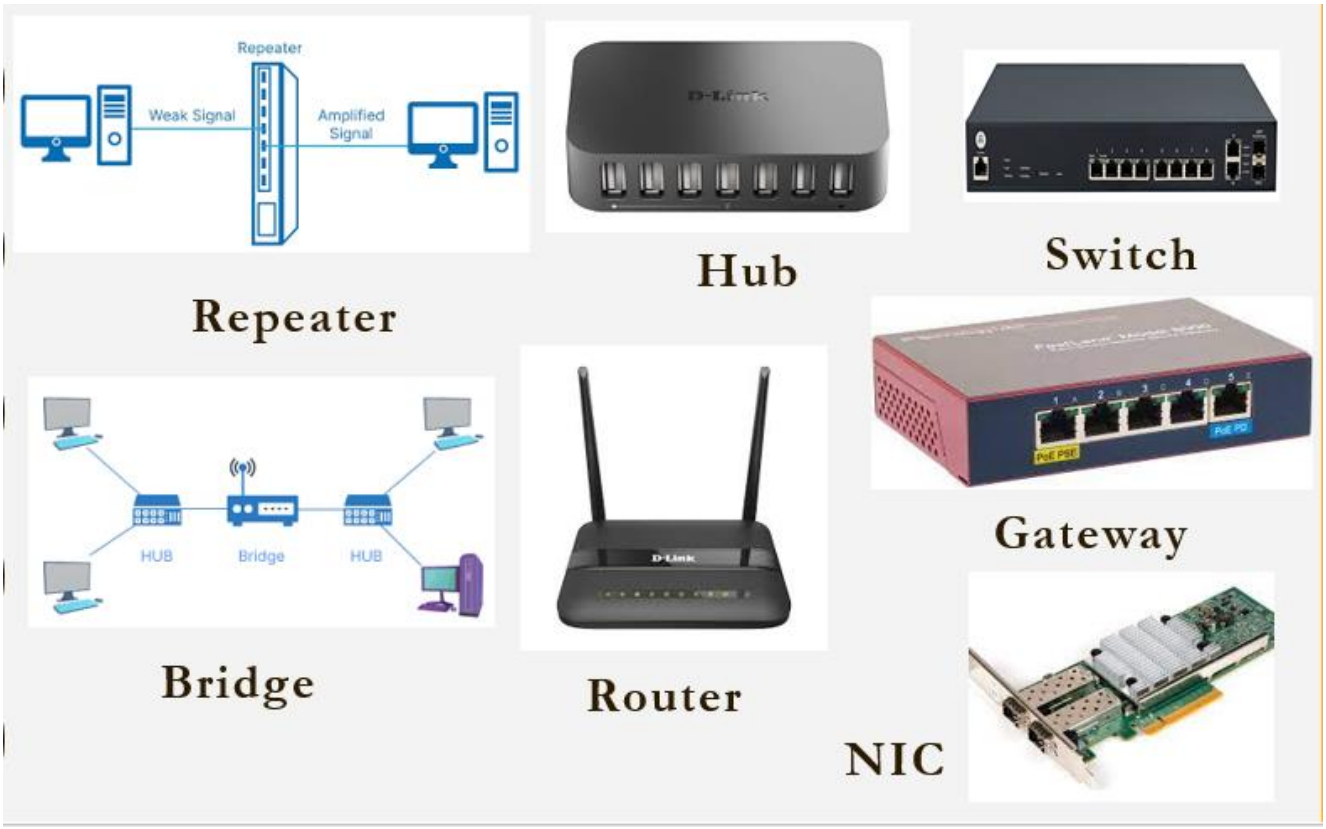

Figure 4.7: Networking Devices

OSI Model:

OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer. OSI consists of seven layers, and each layer performs a particular network function. OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications. OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task. Each layer is self-contained, so that task assigned to each layer can be performed independently.

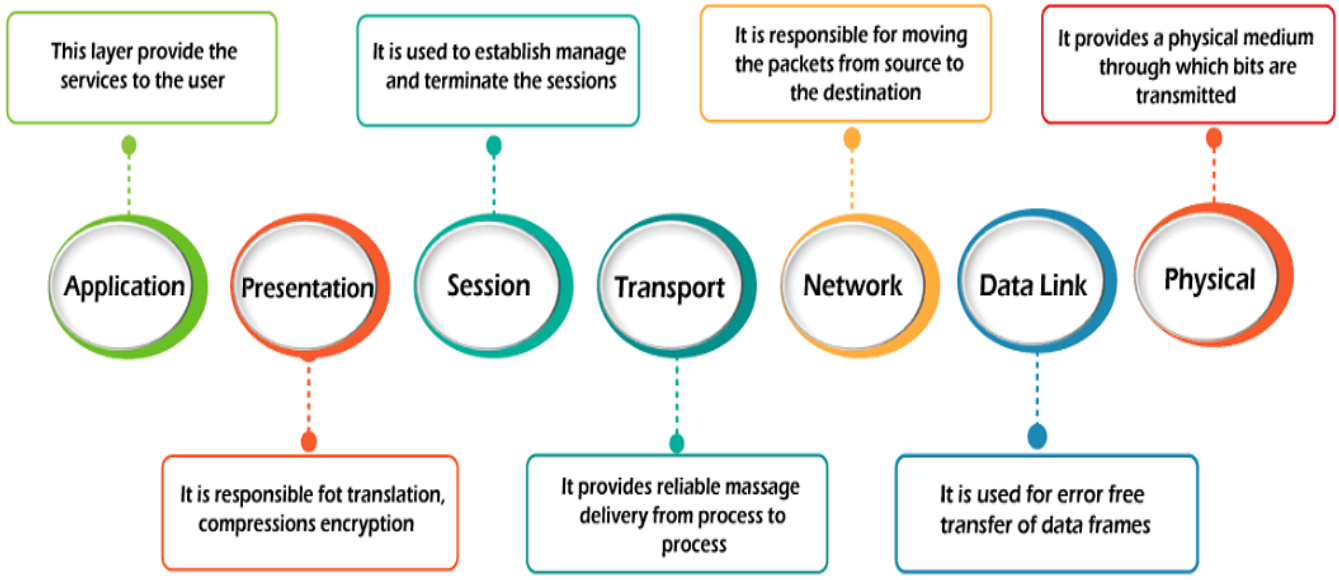

Figure 4.8: OSI Model Layers

Physical Layer: The main functionality of the physical layer is to transmit the individual bits from one node to another node. It is the lowest layer of the OSI model. It establishes, maintains and deactivates the physical connection. It specifies the mechanical, electrical and procedural network interface specifications.

Data Link Layer: This layer is responsible for the error-free transfer of data frames. It defines the format of the data on the network. It provides a reliable and efficient communication between two or more devices. It is mainly responsible for the unique identification of each device that resides on a local network.

Network Layer: It is a layer 3 that manages device addressing, tracks the location of devices on the network. It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors. The Data link layer is responsible for routing and forwarding the packets. Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork. The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Transport Layer: The Transport layer ensures that messages are transmitted in the order in which they are sent and there is no duplication of data. The main responsibility of the transport layer is to transfer the data completely. It receives the data from the upper layer and converts them into smaller units known as segments. This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

Session Layer: The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

Presentation Layer: A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems. It acts as a data translator for a network. This layer is a part of the operating system that converts the data from one presentation format to another format. The Presentation layer is also known as the syntax layer.

Application Layer: An application layer serves as a window for users and application processes to access network service. It handles issues such as network transparency, resource allocation, etc. This layer provides the network services to the end-users.

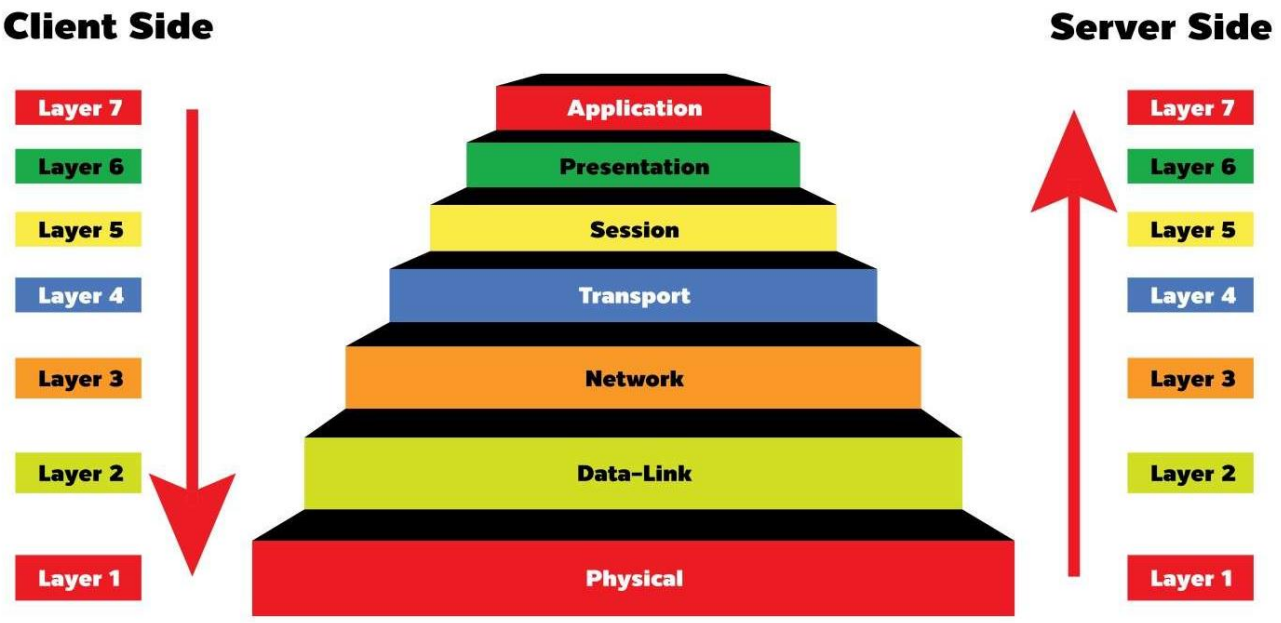

Figure 4.9: OSI Model Client-Server Side

TCP/IP Model

The OSI Model, we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.

TCP/IP was designed and developed by the Department of Defense (DoD) in the 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike the seven layers in the OSI model. The number of layers is sometimes referred to as five or four. The Physical Layer and Data Link Layer are referred to as one single layer as the 'Physical Layer' or 'Network Interface Layer' in the 4-layer reference.

What does TCP/IP Do:

- The main work of TCP/IP is to transfer the data of a computer from one device to another.
- The main condition of this process is to make data reliable and accurate so that the receiver will receive the same information which is sent by the sender.
- To ensure that, each message reaches its final destination accurately, the TCP/IP model divides its data into packets and combines them at the other end, which helps in maintaining the accuracy of the data while transferring from one end to another end.

Physical Layer: It is a group of applications requiring network communications. This layer is responsible for generating the data and requesting connections. It acts on behalf of the sender and the Network Access layer on the behalf of the receiver.

Internet Layer: This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for the logical transmission of data over the entire network. The main protocols residing at this layer are as follows:

- **IP:** IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers.

- **ICMP:** ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
- **ARP:** ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address.

Transport Layer: The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error.

- **TCP:** Applications can interact with one another using TCP as though they were physically connected by a circuit. TCP transmits data in a way that resembles character-by-character transmission rather than separate packets. A starting point that establishes the connection, the whole transmission in byte order, and an ending point that closes the connection make up this transmission.
- **UDP:** The datagram delivery service is provided by UDP, the other transport layer protocol. Connections between receiving and sending hosts are not verified by UDP. Applications that transport little amounts of data use UDP rather than TCP because it eliminates the processes of establishing and validating connections.

Application Layer: This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The three main protocols present in this layer are:

- HTTP and HTTPS
- SSH
- NTP

TCP/IP	**OSI**
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP uses both the session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP follows connectionless a horizontal approach.	OSI follows a vertical approach.
The Transport layer in TCP/IP does not provide assurance delivery of packets.	In the OSI model, the transport layer provides assurance delivery of packets.
Protocols cannot be replaced easily in TCP/IP model.	While in the OSI model, Protocols are better covered and are easy to replace with the technology change.
TCP/IP model network layer only provides connectionless services.	Connectionless and connection-oriented services are provided by the network layer in the OSI model.

Table 4.1: Difference between OSI & TCP/IP

Internet

Internet is a global communication system that links together thousands of individual networks. It allows exchange of information between two or more computers on a network. Thus, internet helps in transfer of messages through mail, chat, video & audio conference, etc. It has become mandatory for day-to-day activities: bills payment, online shopping and surfing, tutoring, working, communicating with peers, etc. Internet was evolved in 1969, under the project called ARPANET (Advanced Research Projects Agency Network) to connect computers at different universities and U.S. defense.

Advantages of Internet	Disadvantages of Internet
It provides great Accessibility to information.	Sometimes, the internet gives Complexity and False Information.
It inculcates easy and faster communication.	Unavailability in bad weather.
People would gain knowledge and obtain loads of information about services.	It leads to the insecurity of information and data loss.
It permits online payments and digital marketing.	It has a bigger Workload and Complex Designing.
It is efficient for business & organizational growth.	It is very expensive when done at the organizational level.
It leads to mass communication among people to spread awareness.	It produces more threats, cyber-attacks, harassment, and violations.
It facilitates social networks to increase development and collaboration.	Increase hate and fake information which can lead to mental health issues.
It provides more security in the banking sector and feasible solutions to issues.	Reliability and security are there, but as the internet is public and worldwide connected, there are chances that issues (viruses, threats) can occur.

Table 4.2: Advantages & Disadvantages of Internet

World Wide Web

The World Wide Web (WWW) or web is an internet-based service, which uses common set of rules known as protocols, to distribute documents across the Internet in a standard way. A collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device. The Web is viewed through web browser software such as Google chrome, Internet Explorer, Mozilla Firefox etc.

E-Commerce

Electronic commerce (ecommerce) refers to companies and individuals that buy and sell goods and services over the Internet. Ecommerce operates in different types of market segments and can be conducted over computers, tablets, smartphones, and other smart devices. Nearly every imaginable product and service is available through ecommerce transactions, including books, music, plane tickets, and financial services such as stock investing and online banking. The business transactions occur either as business-to-business (B2B), business-to-consumer (B2C), consumer-to-consumer or consumer-to-business.

E-Commerce Model: B2B

A website following the B2B business model sells its products to an intermediate buyer who then sells the product to the final customer. As an example, a wholesaler places an order from a company's website and after receiving the consignment, sells the end product to the final customer who comes to buy the product at one of its retail outlets.

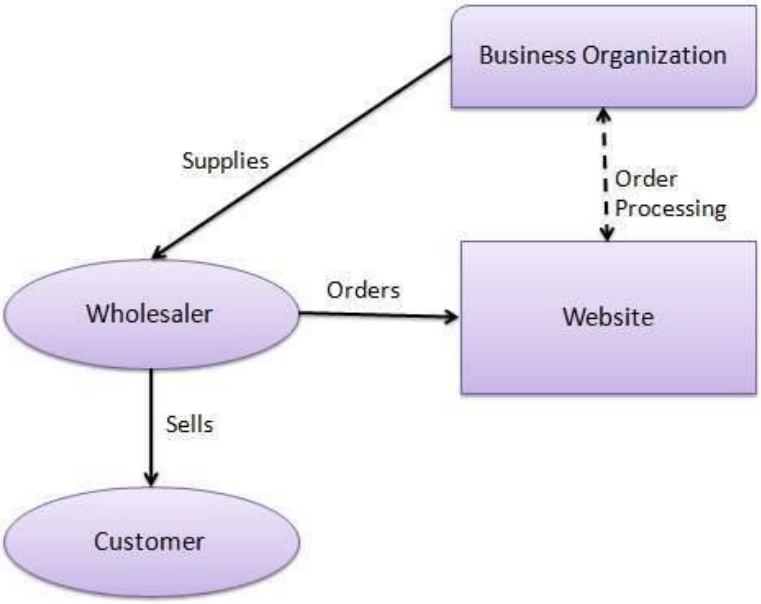

Figure 4.10: B2B Model

E-Commerce Model: B2C

A website following the B2C business model sells its products directly to a customer. A customer can view the products shown on the website. The customer can choose a product and order the same. The website will then send a notification to the business organization via email and the organization will dispatch the product/goods to the customer.

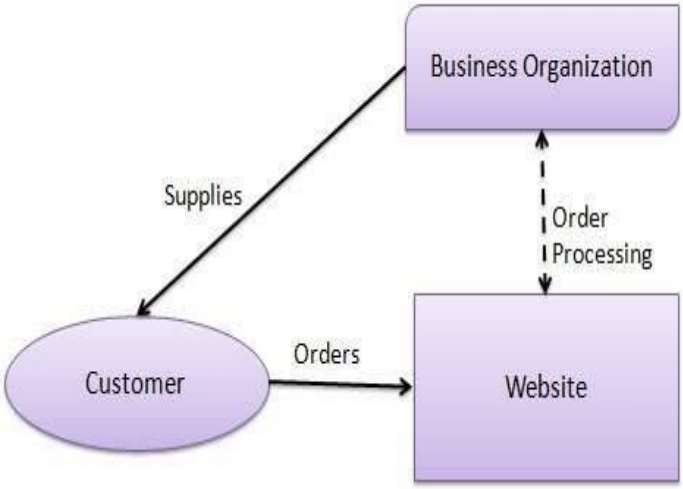

Figure 4.11: B2C Model

E-Commerce Model: C2C

A website following the C2C business model helps consumers to sell their assets like residential property, cars, motorcycles, etc., or rent a room by publishing their information on the website. Website may or may

not charge the consumer for its services. Another consumer may opt to buy the product of the first customer by viewing the post/advertisement on the website.

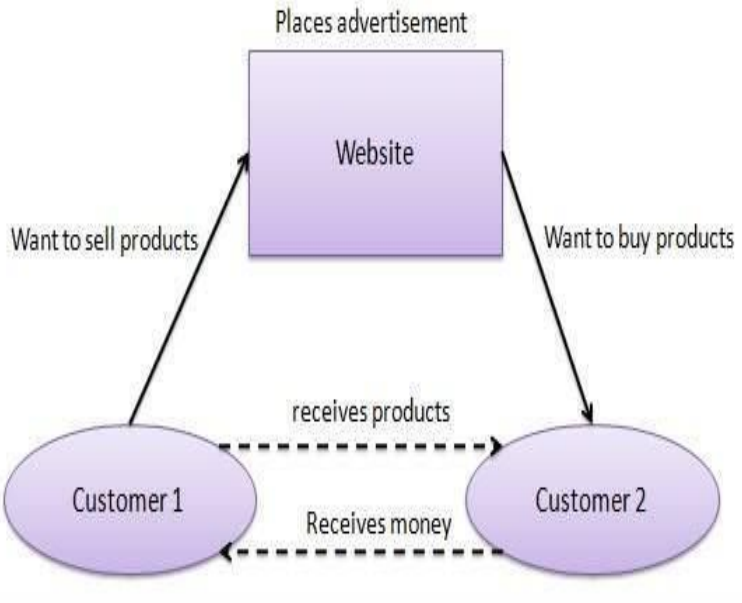

Figure 4.12: C2C Model

Computer Virus

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code into those programs. If this replication succeeds, the affected areas are then said to be "infected" with a computer virus, a metaphor derived from biological viruses. Computer viruses generally require a host program. The virus writes its own code into the host program. When the program runs, the written virus program is executed first, causing infection and damage.

Virus: Vital Information Resources under Siege.

It refers to the type of malicious software that can cause damage to your data, files, and software through replication.

Worms

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers. When these new worm-invaded computers are controlled, the worm will continue to scan and infect other computers using these computers as hosts, and this behavior will continue. Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on exploiting the advantages of exponential growth, thus controlling and infecting more and more computers in a short time. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Malware

"Malware" is short for malicious software and used as a single term to refer to virus, spy ware, worm etc. Malware is designed to cause damage to a stand-alone computer or a networked PC. So wherever a malware term is used it means a program which is designed to damage your computer it may be a virus, worm or Trojan.

Trojan

A Trojan horse is not a virus. It is a destructive program that looks as a genuine application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. Trojans also open a backdoor entry to your computer which gives malicious users/programs access to your system, allowing confidential and personal information to be theft.

Spyware

Spyware is a type of program that is installed with or without your permission on your personal computers to collect information about users, their computer or browsing habits tracks each and everything that you do without your knowledge and send it to remote user. It also can download other malicious programs from internet and install it on the computer. Spyware is usually a separate program that is installed unknowingly when you install another freeware type program or application.

Anti Spyware Software

Anti-spyware software is a type of program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed. Detection may be either rules-based or based on downloaded definition files that identify currently active spyware programs. Anti-spyware products are available from a number of vendors, including Sunbelt Software, TrendMicro and Webroot.

Money Laundering

Money laundering is the process of illegally concealing the origin of money, obtained from illicit activities such as drug trafficking, corruption, embezzlement or gambling, by converting it into a legitimate source. It is a crime in many jurisdictions with varying definitions. It is usually a key operation of organized crime. Money laundering involves disguising financial assets so they can be used without detection of the illegal activity that produced them. Through money laundering, the criminal transforms the monetary proceeds derived from criminal activity into funds with an apparently legal source.

Information Theft

Data theft, also known as information theft, is the illegal transfer or storage of personal, confidential, or financial information. This could include passwords, software code or algorithms, and proprietary processes or technologies. Data theft is considered a serious security and privacy breach, with potentially severe consequences for individuals and organizations. Data theft is the act of stealing digital information stored on computers, servers, or electronic devices to obtain confidential information or compromise privacy. Credit card number theft, ATM spoofing, PIN capturing, database theft, electronic cash are the categories of information theft.

Cyber Pornography

Cyber pornography plays an accessory role in negative social issues such as child abuse, violence against women, inequality, relationship and family breakdown, youth crime. Cyberspace and the pornographic matter transmitted through it have created challenges for India's antiquated laws. The lack of jurisdictional boundaries and the sheer volume of traffic that the Internet can handle, as well as the potential for anonymity have resulted in a complete lack of control over what appears on the Web at the click of a mouse button. Before there was no liability of a cyber café owner but with the introduction of the

Information Technology Amendment Act, 2008, the responsibilities of Cyber Café owners have only increased.

Email Spoofing

Email spoofing is a threat that involves sending email messages with a fake sender address. Email protocols cannot, on their own, authenticate the source of an email. Therefore, it is relatively easy for a spammer or other malicious actors to change the metadata of an email. This way, the protocols think it came the real sender. Email spoofing takes advantage of the fact that email, in many ways, is not very different from regular mail. Each email has three elements: an envelope, a message header, and a message body. An email spoofer puts whatever they want into each of those fields, not just the body and "To:" fields. This means they can customize the information in the following fields: Mail from, Reply to, From, Subject, Date, To.

Denial of Service

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e. employees, members, or account holders) of the service or resource they expected. Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle.

Cyber Stalking

Cyberstalking is a type of cybercrime that uses the internet and technology to harass or stalk a person. It can be considered an extension of cyberbullying and in-person stalking. However, it takes the form of text messages, e-mails, social media posts, and other mediums and is often persistent, deliberate, and methodical. Some common characteristics of Cyberstalking behavior are tracking locations, breaching data privacy, monitoring online and real-world activities, obsessively tracking the victims' whereabouts, intimidating victims, etc. Social media stalking may include sending threatening private messages or faking photos.

Logic Bomb

A logic bomb is a type of malware that contains malicious code that is discreetly installed into software, a computer network, or an operating system with the goal of causing harm to a network when certain conditions are met. It is triggered at a specific event and used to destroy a system by clearing hard drives, deleting files, or corrupting data. An event can be a specific date or time leading up to the launch of an infected software application or the deletion of a specific record from a system. In order to maximize damage before being noticed, logic bombs are mainly used with trojan horses, worms, and viruses. The primary objective of logic bombs is to reformat a hard drive, modify or corrupt data, and remove important files from the system.

Hacking

Act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and

data theft by cyber criminals. Hacking in cyber security refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity. A traditional view of hackers is a lone rogue programmer who is highly skilled in coding and modifying computer software and hardware systems. They are also highly skilled in creating attack vectors that trick users into opening malicious attachments or links and freely giving up their sensitive personal data.

Spamming

Spamming is the use of electronic messaging systems like e-mails and other digital delivery systems and broadcast media to send unwanted bulk messages indiscriminately. The term spamming is also applied to other media like in internet forums, instant messaging, and mobile text messaging, social networking spam, junk fax transmissions, television advertising and sharing network spam. Spam- Unwanted “junk” e-mail sent to a large number of people to promote products or services. The people that create electronic spam are called spammers. Spamming is economically viable because advertisers have very little operating costs beyond the management of their mailing lists. Spammers frequently use false names, address, phone numbers and other contact information to setup disposable accounts at various Internet service providers.

Cyber Defamation

The tremendous development and rapid growth in technology have brought about a drastic change in today's world. Through social networking sites, things like communication or access to information are now made easier through the internet. With the advent of the internet and technology, crimes in cyberspace have raised to a greater extent. The foremost reasons for such activities include an easy approach to the act and the feasibility because the internet is the cheapest way of communication made through text, photographs, audio, and videos.

The risk of "Cyber Defamation" has increased as a result of sharing, posting, and commenting on content on several social networking sites and it not only affects the reputation of an individual, but sometimes the whole community. As per black's law dictionary, defamation means, "the offense of injuring a person's character, fame, or reputation by false and malicious statements". The wrongdoer intends to damage the reputation of another person by making a defamatory statement. While in the case of cyber defamation not only includes verbal or written communications but also includes statements made in cyberspace through the internet. In short, defaming a person through a virtual medium is known as "Cyber Defamation".

Firewall

A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

Accept: allow the traffic

Reject: block the traffic but reply with an “unreachable error”

Drop: block the traffic with no reply

A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet. Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic. Rules can be defined on the firewall based on the necessity and security policies of the organization. From the perspective of a server, network traffic can

be either outgoing or incoming. Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication. Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP.

Computer Ethics

Ethics are actually the unwritten code of conduct that every individual should follow. These codes are considered correct only by the members of that particular profession. Similarly, for computer users, computer ethics is a set of principles that regulates the use of computers. Computer ethics address issues related to the misuse of computers and how they can be prevented. It primarily imposes the ethical use of computing resources. It includes methods to avoid violating the unauthorized distribution of digital content.

Computer Ethics

The core issues surrounding computer ethics are based on the use of the internet, internet privacy, copyrighted content, software, and related services, and user interaction with websites. The Internet has changed our lifestyle. It has become a part of our life. It allows us to communicate with a person from another part of the world. Collecting information on any topic, social meets, and many other activities. But at the same time, some peoples are always trying to cheat or harm others.

The commandments of computer ethics are as follows:

- Do not use the computer to harm other people's data.
- Do not use a computer to cause interference in other people's work.
- Do not spy on another person's personal data.
- Do not use technology to steal personal information.
- Do not spread misinformation using computer technology.
- Do not use the software unless you pay for this software.
- Do not use someone else's computer resources unless he authorized to use them.
- It is wrong to claim ownership of a work that is the output of someone else's intellect.
- Before developing software, think about the social impact it can of that software.
- While computers for communication, always respectful with fellow members.

Cyber Laws

Cyber laws are framework draft by government to take action against Cyber Crime. Cyber laws of Govt. of India are knowns as Information Technology Act 2000 (IT act 2000) which provides way to deal with cybercrime such as hacking, Virus/Worm attacks, DoS attack, credit / debit card fraud. This law ensures people to carried out on-line transaction or communication fearlessly without being cheated for victim. Therefore, Cyber laws or Internet laws regulate Cyber Crime.

Computer Security Habits

Install anti-spyware products.

Make sure your computer has good strong password.

Patch your machine regularly.

Use an anti-virus product and update it regularly.

If possible, use a router-based firewall.

Check for security patches and software updates. Microsoft and other popular operating systems offer regular updates and software patches to protect against viruses and security flaws. Make sure your computer regularly checks for updates or visit the appropriate web page to get the latest download. (Windows users can get security updates.

Change your passwords. Change your passwords regularly, particularly for financially sensitive accounts and web sites. Don’t use the same password for multiple accounts. Do not keep a copy of all your passwords on your computer. It will be much harder to re-create or access accounts if data is lost.

Back up your data. Set aside a few minutes a week to back up your files and personal data.