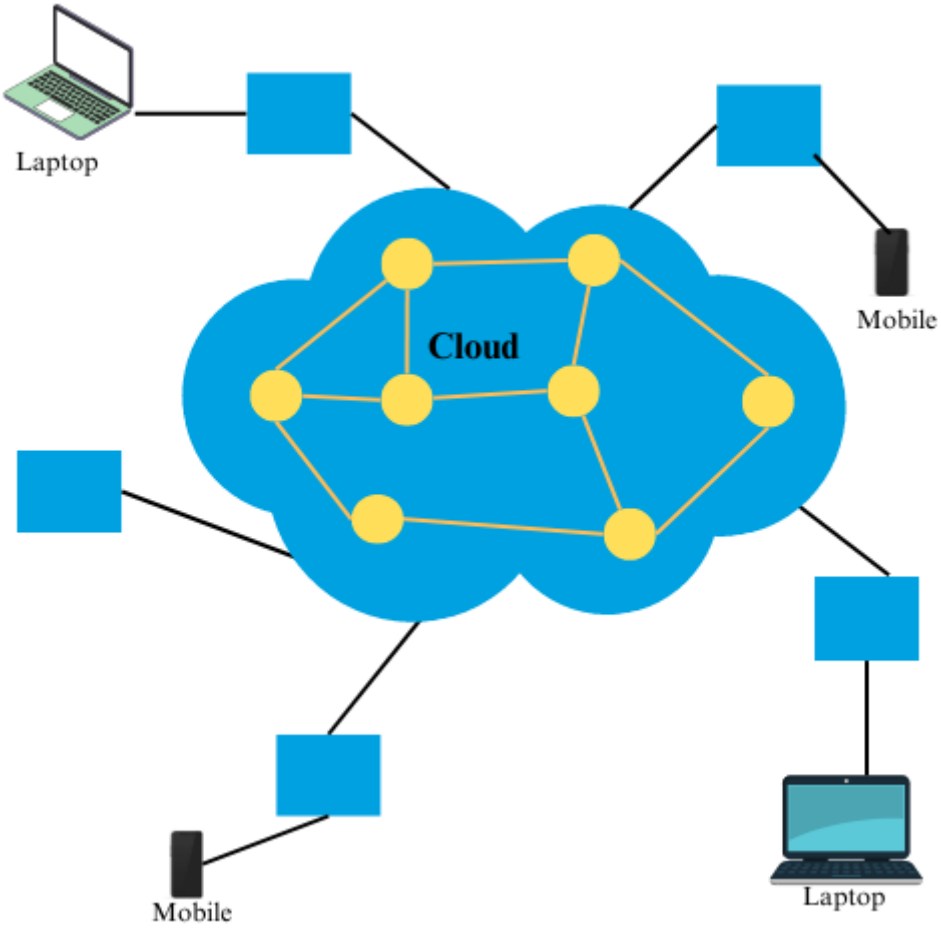
SEC 381:
UNIT 1:

What is Cyberspace?

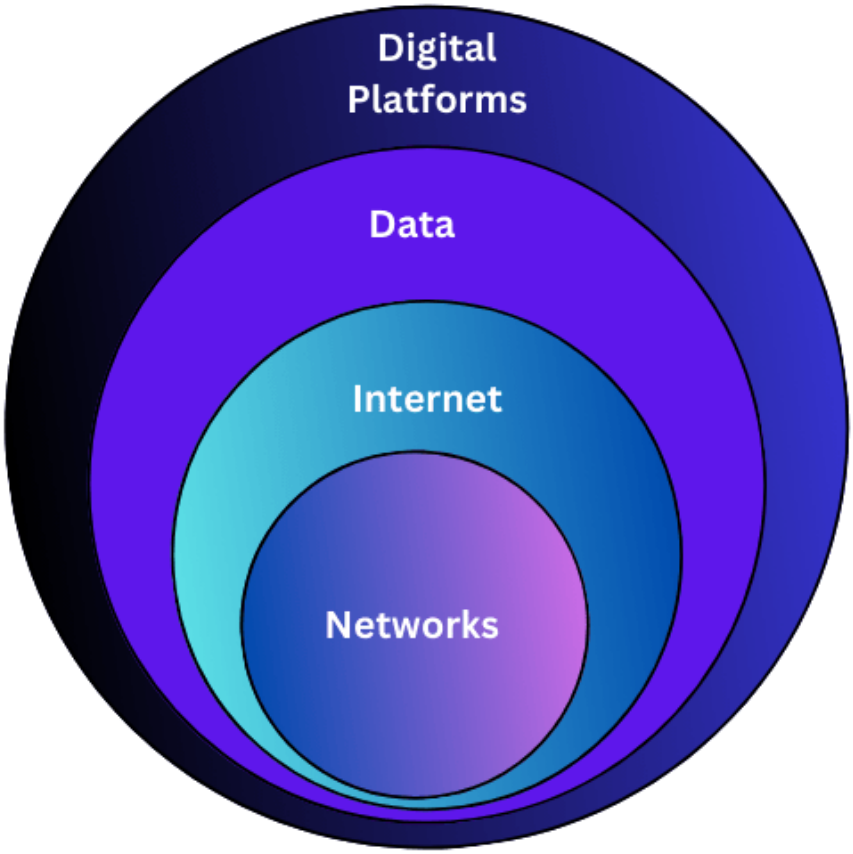
Cyberspace is termed as a virtual and dynamic domain created by computer clones. Cyberspace best describes the immaterial space where interactions through digital networks, the internet, and computer systems take place. Firstly began by sci-fi pioneer William Gibson writing in his 1984 novel "Neuromancer" and then subsequently looking forward to a virtual reality where users were capable of moving through 3-dimensional digital spaces, cyberspace was initially developed in the early nineties. While the concept has matured over time, its essence remains consistent, an area of making a tiny realm of human faculties prone to technology. Cyberspace is fundamentally dependent on technical advancement and innovation. All digital interactions in this space, including sending emails, visiting websites, and using social media are part of cyberspace.



Cyberspace

Components of Cyberspace

Here are some of the components of cyberspace that are as follows:



Major Components of Cyberspace

- Networks: The basis of cyberspace is computer network architecture consisting of access networks, MANs, and WANs that often extend to devices operating as channels through which data are relayed. These networks may involve a great radius as in the case of single buildings or astronomically long distances as is the case with space-based networks. They may employ media as diverse as electrical cables, wirelines to switching nodes and bridges as well as spanning the whole universe.
- The Internet: Mainly among the various features of this phenomenal space of cyberspace the Internet is undoubtedly the most remarkable, a complex structure of structures essentially used as a communication channel for the distribution of information & also online business platforms. The internet is like a mixture of cyberspace that has websites where messages are sent and stuff for entertainment purposes like online games and social networks.
- Data: It is data that guarantees the magnetic Connections of the peoples of Cyberspace. Information is rushing over the net at billions of bits per second. Data as a whole has many different formats that can be written, images, videos, or files. It would be virtually impossible to expect any online activity undertaken without data being exchanged or compromised.
- Digital Platforms: It`s a virtual world that exists in the form of digital as well as online systems that provide services, as well as resources via active interaction. Such a digital suitcase incorporating social media and search platforms as well

as cloud storage and online marketplace is the building block of the framework of the digital world.

Characteristics of Cyberspace

Here are some of the key characteristics of cyberspace, which include:

- **Borderless:** While contrasting with real-world areas being strictly separated by geographic boundaries, cyberspace is beyond classifications and does not have consideration of geographic location in its connectivity instantaneously. This borderless condition creates a high level of international cooperation as a positive side and can raise many of the challenges to cybersecurity as a disadvantage.
- **Dynamic:** Cyberspace is characterized by high strength, arising from technological innovations, among the people who access it, and the legal frameworks. Culture appears on the scene in a flash, old technologies keep getting updated, and the threat of cyber-attacks continuously renews itself and lays new and new challenges as the digital space changes around the clock.
- **Accessible:** The cyberspace idea is the comparison of it with the inhabitants of Earth, in that anyone with an internet connection can gain access to the information and resources that would supposedly go for a long period without others. However, the overall national level of digital infrastructure, social factors, and governmental constraints are the possible issues for reaching the space of cyber for some populations.
- **Anonymous:** The users of the internet cannot be identified in the digital space because the anonymity of virtual presence allows them to know privately without disclosing their real names. Whilst on one side, anonymity can mean privacy and defense, it can also offer a great chance for bad guys to commit web crime like cybercrimes and online harassment.

Challenges and Considerations

Cyberspace presents an array of challenges and considerations that are as follows:

- **Cybersecurity:** The cyber-realm breeds its intensity-in-scale dangers, with the increase in the use of malware, phishing attacks, data leakages, and cyber wars. Shielding the computerized info and Maintaining online safety is still an ongoing issue for people, enterprises, and governments.
- **Privacy:** The obtaining and the proper use of personal information not within physical space can be considered the main problem that is connected to privacy. For instance, data tracking, data surveillance, and unauthorized usage of personal data ask for the implementation of necessary data privacy controls.
- **Digital Divide:** Unequal access to the net and computer literacy as well as less information contribute to the formation of the chess paradigm meaning that those people who don't have enough resources and expertise to utilize the cyber world fully are excluded from these processes. Bridging this gap is a foremost priority for giving everyone the same chance to fully benefit from digital opportunities and a more equal platform.
- **Regulation and Governance:** The undefinable scope of online activities and access to electronic spaces creates a huge problem for government circles as there are no clear rules to govern them. It is vital, at the same time, to maintain freedom of speech prevailing over the Net, yet some boundaries should be set up with no excessive limitation. Policymakers and digital platforms have a great

challenge to fight against the negative content that goes beyond the liberality principle and proscribed acts.

Cryptography and its Types

Cryptography is technique of securing information and communications through use of codes so that only those persons for whom the information is intended can understand it and process it. Thus, preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”.
In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography:

In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

1. Confidentiality:
Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. Integrity:
Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. Non-repudiation:
The creator/sender of information cannot deny his or her intention to send information at later stage.
4. Authentication:
The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Types Of Cryptography:

In general there are three types of cryptography:
1. Symmetric Key Cryptography:
It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but

the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System (DES).

2. Hash Functions:

There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.

3. Asymmetric Key Cryptography:

Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

Message Security:

Security Provides following services:

1. Privacy
2. Authentication
3. Integrity
4. Non repudiation

Privacy: User and Sender expect confidentiality

1. The message must be encrypted
2. A good privacy technique guarantees that intruder (eavesdropper) can't understand the contents of the message
3. Privacy can be achieved with the help of
4. Symmetric-key encryption
5. or
6. Public-Key encryption

Authentication:

1.Receiver needs to be sure that an imposter has not sent the message

2. Digital signature can provide message authentication

Integrity:

1. Data must arrive at the receiver exactly as they were sent
2. No change during transmission either advertently or inadvertently
3. It must be preserved in a secure communication
4. Digital signature is a method that provide message integrity.

Non-Repudiation

1. Receiver must be able to prove that a received message came from a

specific sender
2. Sender or receiver can't deny the transaction
3. The burden of proof falls on the receiver
4. Digital signature provides the support of non-repudiation

Cryptography:

Cryptography is the art and science of decryption for the purpose of secrecy or authenticity.
It facilitates the **secure storage and transmission** of critical data in an **insecure network**.
cryptography is a process of using electronic security systems, methods, and schemes
It **protects data by altering it in a way so that only the intended recipient is able to extract the original** information.

It uses two mechanism known as **encryption and decryption.**

Security solutions:

There are two types of cryptographies
1. **private key cryptography**
2. **Public key cryptography**

Private key or symmetric key cryptography

This type of cryptography involves the usage of a shared key for both encryption and decryption by the sender and the receiver respectively. For each pair of sender and receiver, there is a shared key. One sender may have a set of shared keys with say "n" receivers.
The shared key must be distributed to both the parties very securely before the transmission occurs and should be kept secret for the particular pair of sender and receiver.

Private key or symmetric key cryptography:

The sender sends the message by encrypting it with his shared key to the receiver. On receiving the message, the receiver checks the header to identify the sender.
This is done because a receiver may have a **pair of shared keys** with **"n" users** so he needs to identify from which person it is arriving. He has an electronic key storage area from where he takes out the duplicate of the particular pair and then decrypts the message. This type of cryptography is also **known as the private key cryptography**.

Public key or Asymmetric key cryptography:

This type of cryptography involves the usage of a **pair of private keys and public keys**. Here in this case both the sender and the receiver generates a pair of private key and a public key respectively. Any document **encrypted with the public key** of user X can only be **decrypted by the private key of the user X and vice versa**. So before the transmission

between the sender and the receiver occurs,

1. Sender knows the public key of the receiver
and
2. Receiver knows the public key of the sender.

Public Keys and Trust:

- How are public keys stored?
- How to obtain the public key?
- How does Bob know or 'trusts' that PA is Alice's public key?

Review of Secret Key (Symmetric) Cryptography:

• Confidentiality
– stream ciphers
– block ciphers with encryption modes
• Integrity
– message authentication code
• Limitation: sender and receiver must share the same key
– needs secure channel for key distribution
– impossible for two parties having no prior relationship.

Overview of Computer and Web-technology:

Web Technology

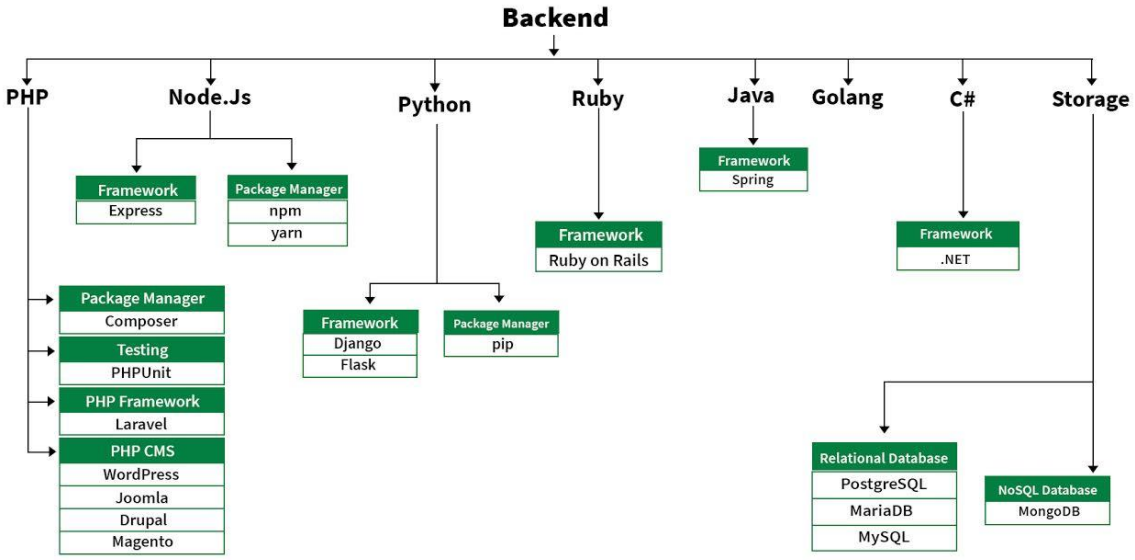
Web Technology refers to the various tools and techniques that are utilized in the process of communication between different types of devices over the Internet. A web browser is used to access web pages. Web browsers can be defined as programs that display text, data, pictures, animation, and video on the Internet. Hyperlinked resources on the World Wide Web can be accessed using software interfaces provided by Web browsers.

Web Technology can be Classified into the Following Sections:

- World Wide Web (WWW): The World Wide Web is based on several different technologies: Web browsers, Hypertext Markup Language (HTML), and Hypertext Transfer Protocol (HTTP).
- Web Browser: The web browser is an application software to explore www (World Wide Web). It provides an interface between the server and the client and requests to the server for web documents and services.
- Web Server: Web server is a program which processes the network requests of the users and serves them with files that create web pages. This exchange takes place using Hypertext Transfer Protocol (HTTP).
- Web Pages: A webpage is a digital document that is linked to the World Wide Web and viewable by anyone connected to the internet has a web browser.
- Web Development: Web development refers to the building, creating, and maintaining of websites. It includes aspects such as web design, web publishing, web programming, and database management. It is the creation of an application that works over the internet i.e. websites.

Web Development can be Classified into Two Ways:

- Frontend Development: The part of a website that the user interacts directly is termed as front end. It is also referred to as the 'client side' of the application.
- Backend Development: Backend is the server side of a website. It is the part of the website that users cannot see and interact. It is the portion of software that does not come in direct contact with the users. It is used to store and arrange data.



Frontend Development Languages

The front-end portion is built by using some languages which are discussed below:

- HTML: HTML stands for Hypertext Markup Language. It is used to design the front-end portion of web pages using a markup language. HTML is the combination of Hypertext and Markup language. Hypertext defines the link between the web pages. The markup language is used to define the text documentation within the tag which defines the structure of web pages.
- CSS: Cascading Style Sheets fondly referred to as CSS is a simply designed language intended to simplify the process of making web pages presentable. CSS allows you to apply styles to web pages. More importantly, CSS enables you to do this independent of the HTML that makes up each web page.
- JavaScript: JavaScript is a famous scripting language used to create magic on the sites to make the site interactive for the user. It is used to enhancing the functionality of a website to running cool games and web-based software.
- AJAX: Ajax is an acronym for Asynchronous Javascript and XML. It is used to communicate with the server without refreshing the web page and thus increasing the user experience and better performance.

There are many other languages through which one can do front-end development depending upon the framework for
example *Flutter* user *Dart*, *React* uses *JavaScript* and *Django* uses *Python*, and much more.

Front End Frameworks and Libraries

HTML

CSS

- CSS Frameworks
    - Bootstrap
    - Tailwind CSS
    - Bulma
    - Foundation
    - Primer CSS
    - Spectre CSS
    - Materialize CSS
    - Onsen UI
    - Semantic UI
    - Blaze UI
    - Pure CSS
    - Tachyons
- CSS Preprocessors
    - SASS
    - LESS

JavaScript

- JavaScript Technology
    - ES6
    - TypeScript
- JavaScript Frameworks
    - AngularJS
        - Angular ngx Bootstrap
        - Angular PrimeNG
        - Angular Material UI
    - VueJS
        - NuxtJS
- JavaScript Libraries
    - jQuery
        - jQuery UI
        - jQuery Mobile
        - jQWidgets
        - jQuery EasyUI
    - ReactJS
        - NextJS
        - Ant Design
        - React Desktop
        - React Rebass
        - React Bootstrap
        - React Reactstrap
        - BlueprintJS
        - React Suite
        - React.js Evergreen
        - React Material UI
    - P5.js
    - Fabric.js

- D3.js
- Collect.js
- Underscore.js
- Lodash
- TensorFlow.js

Backend Development Languages

The back end portion is built by using some languages which are discussed below:

- PHP: PHP is a server-side scripting language designed specifically for web development. Since PHP code executed on the server-side, so it is called a server-side scripting language.
- Node.js: Node.js is an open-source and cross-platform runtime environment for executing JavaScript code outside a browser. You need to remember that NodeJS is not a framework, and it's not a programming language. Most people are confused and understand it's a framework or a programming language. We often use Node.js for building back-end services like APIs like Web App or Mobile App. It's used in production by large companies such as Paypal, Uber, Netflix, Wallmart, and so on.
- Python: Python is a programming language that lets you work quickly and integrate systems more efficiently.
- Ruby: Ruby is a dynamic, reflective, object-oriented, general-purpose programming language. Ruby is a pure Object-Oriented language developed by Yukihiro Matsumoto. Everything in Ruby is an object except the blocks but there are replacements too for it i.e procs and lambda. The objective of Ruby's development was to make it act as a sensible buffer between human programmers and the underlying computing machinery.
- Java: Java is one of the most popular and widely used programming languages and platforms. It is highly scalable. Java components are easily available.
- JavaScript: JavaScript can be used as both (front end and back end) programming.
- Golang: Golang is a procedural and statically typed programming language having the syntax similar to C programming language. Sometimes it is termed as Go Programming Language.
- C#: C# is a general-purpose, modern and object-oriented programming language pronounced as "C sharp".
- DBMS: The software which is used to manage database is called Database Management System (DBMS)

Data Communication – Definition, Components, Types, Channels

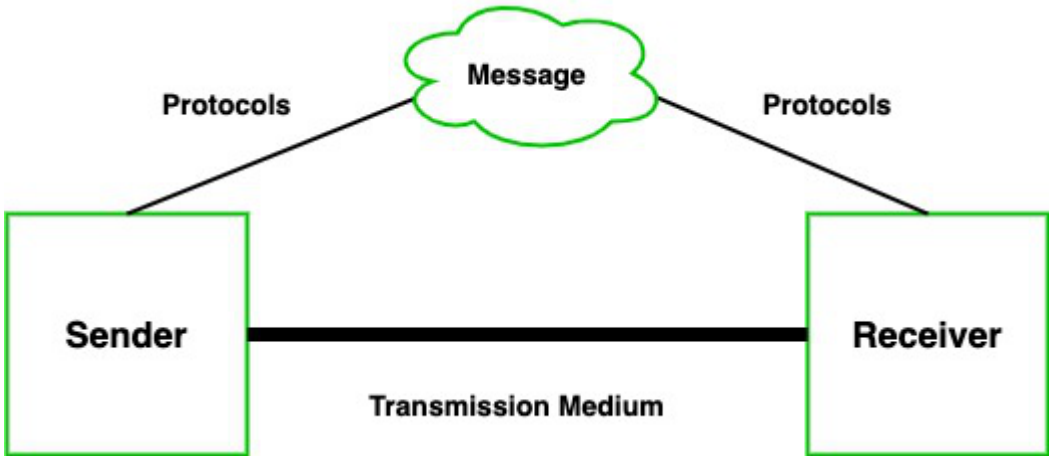
Communication is defined as a process in which more than one computer transfers information, instructions to each other and for sharing resources. Or in other words, communication is a process or act in which we can send or receive data. A network of computers is defined as an interconnected collection of autonomous computers. Autonomous means no computer can start, stop or control another computer.

Components of Data Communication

A communication system is made up of the following components:

1. Message: A message is a piece of information that is to be transmitted from one person to another. It could be a text file, an audio file, a video file, etc.

2. Sender: It is simply a device that sends data messages. It can be a computer, mobile, telephone, laptop, video camera, or workstation, etc.
3. Receiver: It is a device that receives messages. It can be a computer, telephone mobile, workstation, etc.
4. Transmission Medium / Communication Channels: Communication channels are the medium that connect two or more workstations. Workstations can be connected by either wired media or wireless media.
5. Set of rules (Protocol): When someone sends the data (The sender), it should be understandable to the receiver also otherwise it is meaningless. For example, Sonali sends a message to Chetan. If Sonali writes in Hindi and Chetan cannot understand Hindi, it is a meaningless conversation.



Therefore, there are some set of rules (protocols) that is followed by every computer connected to the internet and they are:

- TCP(Transmission Control Protocol): It is responsible for dividing messages into packets on the source computer and reassembling the received packet at the destination or recipient computer. It also makes sure that the packets have the information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination.
- IP(Internet Protocol): Do You ever wonder how computer determines which packet belongs to which device. What happens if the message you sent to your friend is received by your father? Scary Right. Well! IP is responsible for handling the address of the destination computer so that each packet is sent to its proper destination.

Type of data communication

As we know that data communication is communication in which we can send or receive data from one device to another. The data communication is divided into three types:

1. Simplex Communication: It is one-way communication or we can say that unidirectional communication in which one device only receives and another device only sends data and devices uses their entire capacity in transmission. For example, IoT, entering data using a keyboard, listing music using a speaker, etc.
2. Half Duplex communication: It is a two-way communication, or we can say that it is a bidirectional communication in which both the devices can send and receive data but not at the same time. When one device is sending data then another device is only receiving and vice-versa. For example, walkie-talkie.

3. **Full-duplex communication:** It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data at the same time. For example, mobile phones, landlines, etc.

Communication Channels

Communication channels are the medium that connects two or more workstations. Workstations can be connected by either wired media or wireless media. It is also known as a transmission medium. The transmission medium or channel is a link that carries messages between two or more devices. We can group the communication media into two categories:

- Guided media transmission
- Unguided media transmission

1. Guided Media: In this transmission medium, the physical link is created using wires or cables between two or more computers or devices, and then the data is transmitted using these cables in terms of signals. Guided media transmission of the following types:

1. Twisted pair cable: It is the most common form of wire used in communication. In a twisted-pair cable, two identical wires are wrapped together in a double helix. The twisting of the wire reduces the crosstalk. It is known as the leaking of a signal from one wire to another due to which signal can corrupt and can cause network errors. The twisting protects the wire from internal crosstalk as well as external forms of signal interference. Types of Twisted Pair Cable :

- Unshielded Twisted Pair (UTP): It is used in computers and telephones widely. As the name suggests, there is no external shielding so it does not protects from external interference. It is cheaper than STP.
- Shielded Twisted Pair (STP): It offers greater protection from crosstalk due to shield. Due to shielding, it protects from external interference. It is heavier and costlier as compare to UTP.

2. Coaxial Cable: It consists of a solid wire core that is surrounded by one or more foil or wire shields. The inner core of the coaxial cable carries the signal and the outer shield provides the ground. It is widely used for television signals and also used by large corporations in building security systems. Data transmission of this cable is better but expensive as compared to twisted pair.

3. Optical fibers: Optical fiber is an important technology. It transmits large amounts of data at very high speeds due to which it is widely used in internet cables. It carries data as a light that travels inside a thin glass fiber. The fiber optic cable is made up of three pieces:

1. Core: Core is the piece through which light travels. It is generally created using glass or plastic.
2. Cladding: It is the covering of the core and reflects the light back to the core.
3. Sheath: It is the protective covering that protects fiber cable from the environment.

2. Unguided Media: The unguided transmission media is a transmission mode in which the signals are propagated from one device to another device wirelessly. Signals can wave through the air, water, or vacuum. It is generally used to transmit signals in all directions. Unguided Media is further divided into various parts :

1. Microwave: Microwave offers communication without the use of cables. Microwave signals are just like radio and television signals. It is used in long-distance communication. Microwave transmission consists of a transmitter, receiver, and atmosphere. In microwave communication, there are parabolic antennas that are mounted on the towers to send a beam to another antenna. The higher the tower, the greater the range.

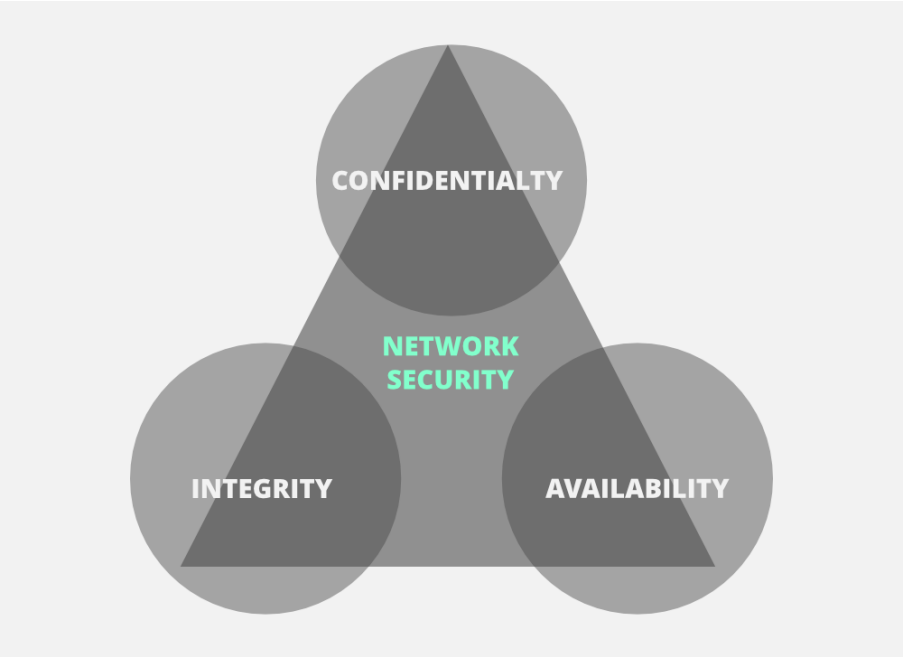
2. Radio wave: When communication is carried out by radio frequencies, then it is termed radio waves transmission. It offers mobility. It is consists of the transmitter and the receiver. Both use antennas to radiate and capture the radio signal.
3. Infrared: It is short-distance communication and can pass through any object. It is generally used in TV remotes, wireless mouse, etc.

CIA Triad

When talking about network security, the **CIA** triad is one of the most important models which is designed to guide policies for information security within an organization.

CIA stands for :

1. Confidentiality
2. Integrity
3. Availability

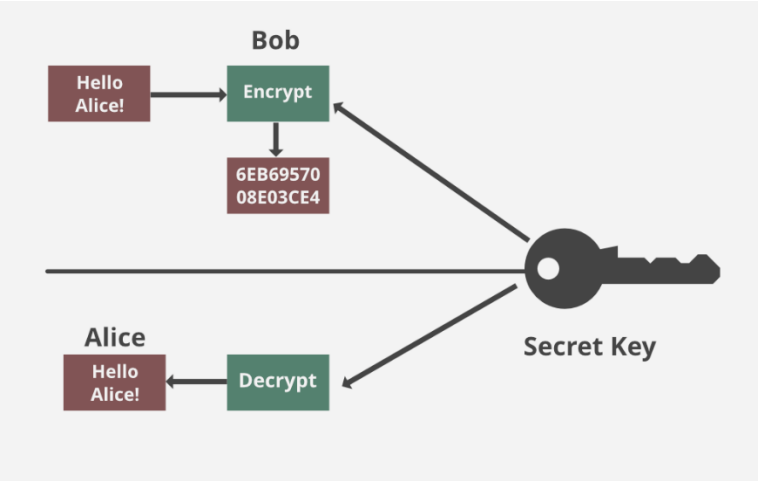


These are the objectives that should be kept in mind while securing a network.

Confidentiality

Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to your information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it. Encryption standards include **AES**(Advanced Encryption Standard) and **DES** (Data Encryption Standard). Another way to protect your data is through a VPN tunnel. VPN stands for Virtual Private Network and helps the data to move securely over

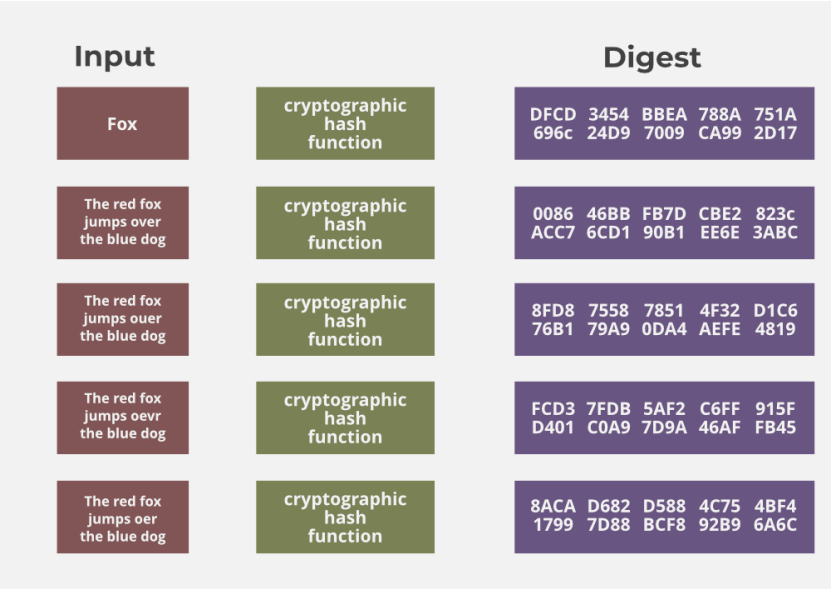
the network.



Integrity

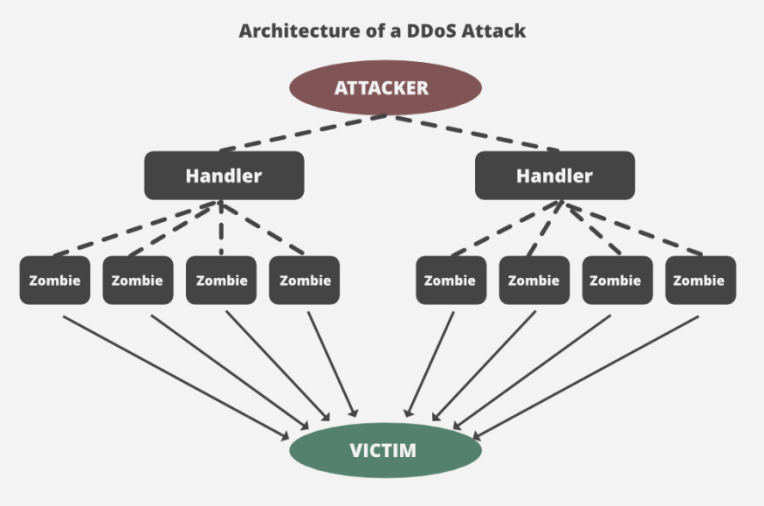
The next thing to talk about is integrity. Well, the idea here is to make sure that data has not been modified. Corruption of data is a failure to maintain data integrity. To check if our data has been modified or not, we make use of a hash function.
We have two common types: SHA (Secure Hash Algorithm) and MD5(Message Direct 5). Now MD5 is a 128-bit hash and SHA is a 160-bit hash if we're using SHA-1. There are also other SHA methods that we could use like SHA-0, SHA-2, and SHA-3.

Let's assume Host 'A' wants to send data to Host 'B' to maintain integrity. A hash function will run over the data and produce an arbitrary hash value H1 which is then attached to the data. When Host 'B' receives the packet, it runs the same hash function over the data which gives a hash value of H2. Now, if H1 = H2, this means that the data's integrity has been maintained and the contents were not modified.



Availability

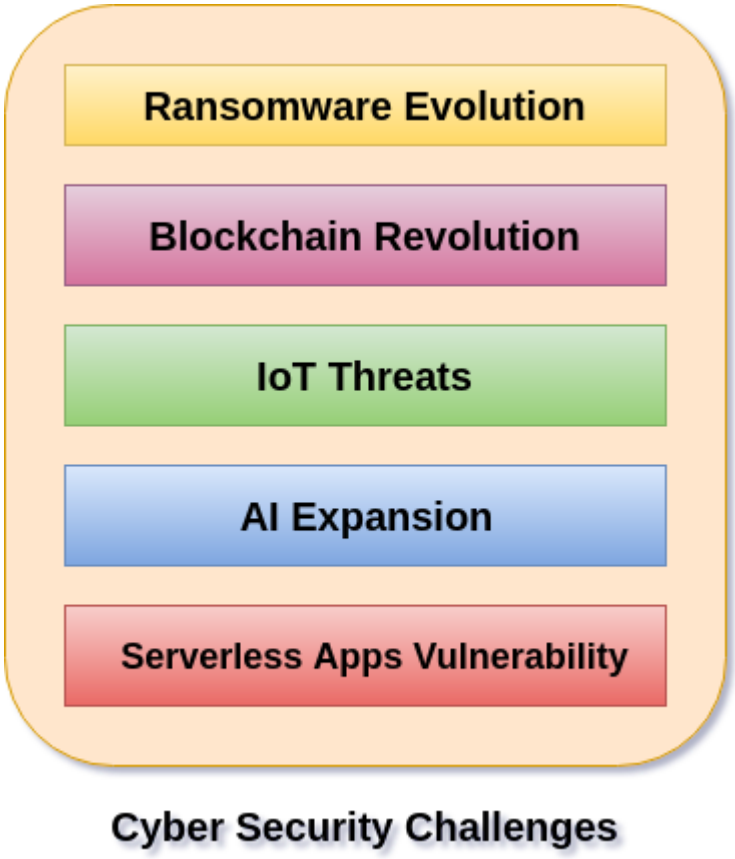
This means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over, and prevent bottlenecks in a network. Attacks such as DoS or DDoS may render a network unavailable as the resources of the network get exhausted. The impact may be significant to the companies and users who rely on the network as a business tool. Thus, proper measures should be taken to prevent such attacks.



Cyber Security Challenges

Today cybersecurity is the main component of the country's overall national security and economic security strategies. In India, there are so many challenges related to cybersecurity. With the increase of the cyber-attacks, every organization needs a security analyst who makes sure that their system is secured. These security analysts face many challenges related to cybersecurity such as securing confidential data of government organizations, securing the private organization servers, etc.

The recent important cybersecurity challenges are described below:



1. Ransomware Evolution

Ransomware is a type of malware in which the data on a victim's computer is locked, and payment is demanded before the ransomed data is unlocked. After successful payment, access rights returned to the victim. Ransomware is the bane of cybersecurity, data professionals, IT, and executives.

Ransomware attacks are growing day by day in the areas of cybercrime. IT professionals and business leaders need to have a powerful recovery strategy against the malware attacks to protect their organization. It involves proper planning to recover corporate and customers' data and application as well as reporting any breaches against the Notifiable Data Breaches scheme. Today's DRaaS solutions are the best defence against the ransomware attacks. With DRaaS solutions method, we can automatically back up our files, easily identify which backup is clean, and launch a fail-over with the press of a button when malicious attacks corrupt our data.

2. Blockchain Revolution

Blockchain technology is the most important invention in computing era. It is the first time in human history that we have a genuinely native digital medium for peer-to-peer value exchange. The blockchain is a technology that enables cryptocurrencies like Bitcoin. The blockchain is a vast global platform that allows two or more parties to do a transaction or do business without needing a third party for establishing trust.

It is difficult to predict what blockchain systems will offer in regards to cybersecurity. The professionals in cybersecurity can make some educated guesses regarding blockchain. As the application and utility of blockchain in a cybersecurity context emerges, there will be a healthy tension but also complementary integrations with traditional, proven, cybersecurity approaches.

3. IoT Threats

IoT stands for Internet of Things. It is a system of interrelated physical devices which can be accessible through the internet. The connected physical devices have a unique identifier (UID) and have the ability to transfer data over a network without any requirements of the human-to-human or human-to-computer interaction. The firmware and software which is running on IoT devices make consumer and businesses highly susceptible to cyber-attacks.

When IoT things were designed, it is not considered in mind about the used in cybersecurity and for commercial purposes. So every organization needs to work with cybersecurity professionals to ensure the security of their password policies, session handling, user verification, multifactor authentication, and security protocols to help in managing the risk.

4. AI Expansion

AI short form is Artificial intelligence. According to John McCarthy, father of Artificial Intelligence defined AI: "The science and engineering of making intelligent machines, especially intelligent computer programs."

It is an area of computer science which is the creation of intelligent machines that do work and react like humans. Some of the activities related to artificial intelligence include speech recognition, Learning, Planning, Problem-solving, etc. The key benefits with AI into our cybersecurity strategy has the ability to protect and defend an environment when the malicious attack begins, thus mitigating the impact. AI take immediate action against the malicious attacks at a moment when a threats impact a business. IT business leaders and cybersecurity strategy teams consider AI as a future protective control that will allow our business to stay ahead of the cybersecurity technology curve.

5. Serverless Apps Vulnerability

Serverless architecture and apps is an application which depends on third-party cloud infrastructure or on a back-end service such as google cloud function, Amazon web services (AWS) lambda, etc. The serverless apps invite the cyber attackers to spread threats on their system easily because the users access the application locally or off-server on their device. Therefore it is the user responsibility for the security precautions while using serverless application.

The serverless apps do nothing to keep the attackers away from our data. The serverless application doesn't help if an attacker gains access to our data through a vulnerability such as leaked credentials, a compromised insider or by any other means then serverless.