- **Security is the process of maintaining an acceptable level of perceived risk**
- Cybersecurity is the protection of Internet-connected systems, including hardware, software, and data from cyber attackers. It is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc.
- It is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification, or unauthorized access. Therefore, it may also be referred to as **information technology security**.
- Cybersecurity is important because it protects you or your company from potential cyber threats. The advancement of technology has left many people vulnerable to cybercriminal activities, such as hacking, data theft and damage, and industrial espionage. Cybercrime rate is increasing; hence, without cyber security, you could lose sensitive information, money, or reputation. Cyber security is as important as the need for technology.
- Information security is a broad field that covers many areas such as physical security, endpoint security, data encryption, and network security. It is also closely related to information assurance, which protects information from threats such as natural disasters and server failures.
- Cybersecurity primarily addresses technology-related threats, with practices and tools that can prevent or mitigate them. Another related category is data security, which focuses on protecting an organization's data from accidental or malicious exposure to unauthorized parties.
- The CIA triad refers to an information security model made up of the three main components: **confidentiality, integrity and availability**. Each component represents a fundamental objective of information security.

Benefits of cybersecurity

- The following are the benefits of implementing and maintaining cybersecurity:
    - Cyberattacks and data breach protection for businesses.
    - Data and network security are both protected.

  - Unauthorized user access is avoided.
  - After a breach, there is a faster recovery time.
  - End-user and endpoint device protection.
  - Regulatory adherence.
  - Continuity of operations.
  - Developers, partners, consumers, stakeholders, and workers have more faith in the company's reputation and trust.

- Security has three features:
  - Integrity
  - Availability
  - Confidentiality

Confidentiality

- Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. Assurance that information is shared only among authorized persons or organizations.
- Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. It prevents essential information from reaching the wrong people. **Data encryption** is an excellent example of ensuring confidentiality.

Integrity

- Assurance that the information is authentic and complete. In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle.

This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event. In addition, it indicates to make the source of information genuine.

Availability

- Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them. Availability of information refers to ensuring that authorized parties are able to access the information when needed.

- This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

Authenticity

- Authenticity refers to the characteristic of a communication, document, or any data that ensures the quality of being genuine .The major role of authentication is to confirm that a user is genuine, one who he / she claims to be. Controls such as bio metrics, smart cards, and digital certificates ensure the authenticity of data, transactions, communications, or documents.

- The user should prove access rights and identity. Commonly, usernames and passwords are used for this method.

- The PKI (Public Key Infrastructure) authentication methodology uses digital certificates to prove a user's identity. Different authentication tools will be key cards or USB tokens. The best authentication threat occurs with unsecured emails that seem legitimate.

Non-Repudiation

- It is the assurance that somebody cannot deny the validity of one thing. It may be a legal thought that's widely used in data security and refers to a service that provides proof of the origin of information and also the **integrity** of the information.

- Non-repudiation makes it very difficult to successfully deny who/where a message came from also as the authenticity of that message.Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message, and that the recipient cannot deny having received the message. Individuals and organization use digital signatures to ensure non-repudiation.

Cryptography and steganography

Cryptography and steganography are the two popular methods available to provide security. Cryptography scrambles a message so it cannot be understood and generates cipher text. Steganography word is derived from Greek, literally means Covered Writing. Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. It includes vast ways of secret communications methods that conceal the messages existence. In Cryptography, the meaning of data has been changed. So, it makes intention to the hacker to hack or destroy the data.

The cryptography and steganography are two extensively used techniques for concealment of data exchange. Cryptography is used to cipher information and steganography is used to hide the reality of data communication. Cryptography scrambles the information by using a key so that a third party cannot access the information without the key.Cryptography is also called as the science of secret script. Steganography hides the information by using a cover medium so that a third person cannot identify the communicationSteganography is also called art and science of writing hidden messages in such a way that no one, except the sender and intended recipient, suspects the existence of the message.[5]Consider any situation wherein a person A, has to send a secret message or some confidential information to another party C through unsecured channels. In this case, it becomes essential to realize the following for secure data transmission:

1. Data Integrity: C should receive the exact message sent by A, it should not be tampered or modified during the transmission.

2. Data Confidentiality: The message should only be received by C and interpretable by C.

3. Authentication: The receiver C should be able to authenticate the sender A and verify that the message has been sent by the desired source.

4. Non-repudiation: The source A should not be in a position to deny the sending of the message. To satisfy the above security services various techniques have been implemented.

Cryptography is the study of mathematical techniques related to characteristics of information security such as confidentiality, authentication, integrity and non-repudiation. The aim of cryptography is to make data unreadable by a third party.

Different Types of Steganography

1. Text Steganography − There is steganography in text files, which entails secretly storing information. In this method, the hidden data is encoded into the letter of each word.

2. Image Steganography − The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

Since the computer description of an image contains multiple bits, images are frequently used as a cover source in digital steganography.

The various terms used to describe image steganography include:

- Cover-Image - Unique picture that can conceal data.
- Message - Real data that you can mask within pictures. The message may be in the form of standard text or an image.
- Stego-Image − A stego image is an image with a hidden message.
- Stego-Key - Messages can be embedded in cover images and stego-images with the help of a key, or the messages can be derived from the photos themselves.

3. Audio Steganography − It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier"). Its typical uses involve media playback, primarily audio clips.

4. Video Steganography − Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

5. Network or Protocol Steganography − It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object. Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

Steganography Examples Include

- Writing with invisible ink
- Embedding text in a picture (like an artist hiding their initials in a painting they've done)
- Backward masking a message in an audio file (remember those stories of evil messages recorded backward on rock and roll records?)
- Concealing information in either metadata or within a file header
- Hiding an image in a video, viewable only if the video is played at a particular frame rate
- Embedding a secret message in either the green, blue, or red channels of an RRB image

Steganography can be used both for constructive and destructive purposes. For example, education and business institutions, intelligence agencies, the military, and certified ethical hackers use steganography to embed confidential messages and information in plain sight.

Types of the cryptography –

Symmetric key cryptography (Secret key cryptography): This type of cryptography uses a key for encrypting and decrypting the plain text and cipher text respectively. The only condition here is that it shares the same key for the encryption and decryption and it also consumes less execution time.

Asymmetric key cryptography (Public key cryptography): This scheme uses two keys named as a private key and public key. The public key is provided by the receiver to the sender to encrypt the message while the private key is applied by the receiver itself to decrypt the message. The keys can be reused with other entities.

Comparison Chart

BASIS FOR COMPARISON	STEGANOGRAPHY	CRYPTOGRAPHY
Basic	It is known as cover writing.	It means secret writing.
Goal	Secret communication	Data protection
Structure of the message	Not altered	Altered only of the transmission.
Popularity	Less popular	More commonly used.
Relies on	Key	No parameters.
Supported security principles	Confidentiality and authentication	Confidentiality, data integrity, authentication, and non-repudiation.
Techniques	Spacial domain, transform domain, model-based and ad-	Transposition, substitution, stream cipher, block ciphers.

	hoc.	
Implemented on	Audio, video, image, text.	Only on text files.
Types of attack	Steganalysis	Cryptanalysis