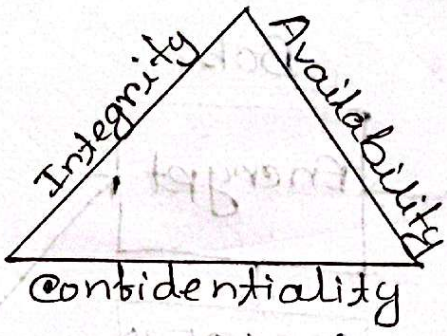
Abida Sultana
IT-21032

1. CIA security goals

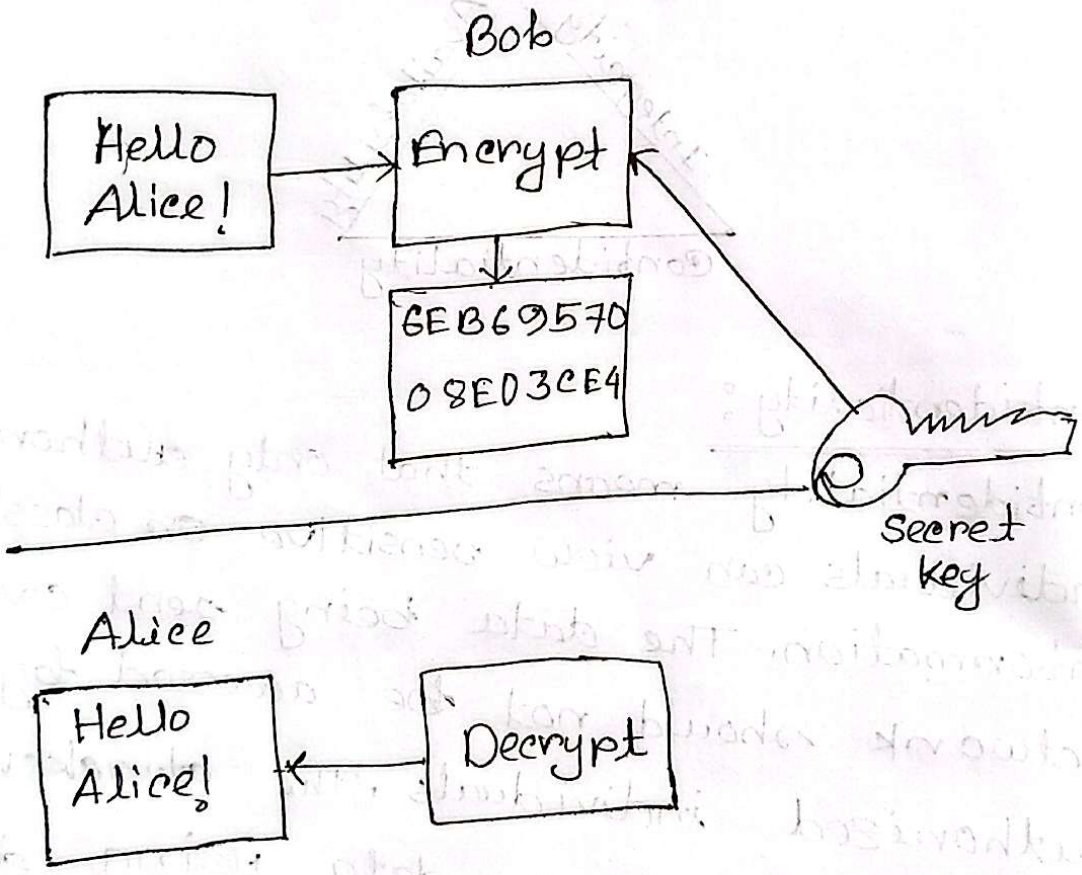
The goals of CIA Triad are confidentiality, Integrity and availability which are basic factors in information security.



Confidentiality :-

Confidentiality means that only authorized individuals can view sensitive or classified information. The data being sent over 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 safegaurd our data so

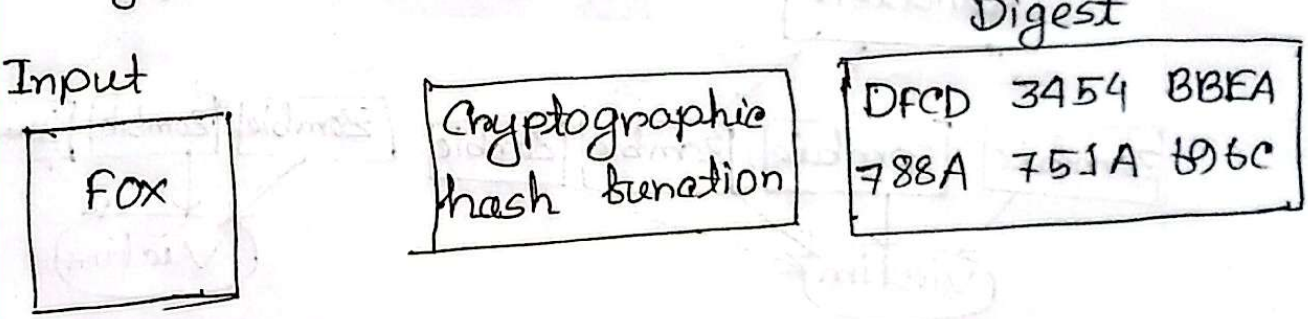
that even if the attacker gains access to our data, he/she will not be able to decrypt it. Another way to protect our data is through a VPN tunnel.



Integrity:

The idea of integrity is to make sure that data has not been modified. Corruption of data is a failure to

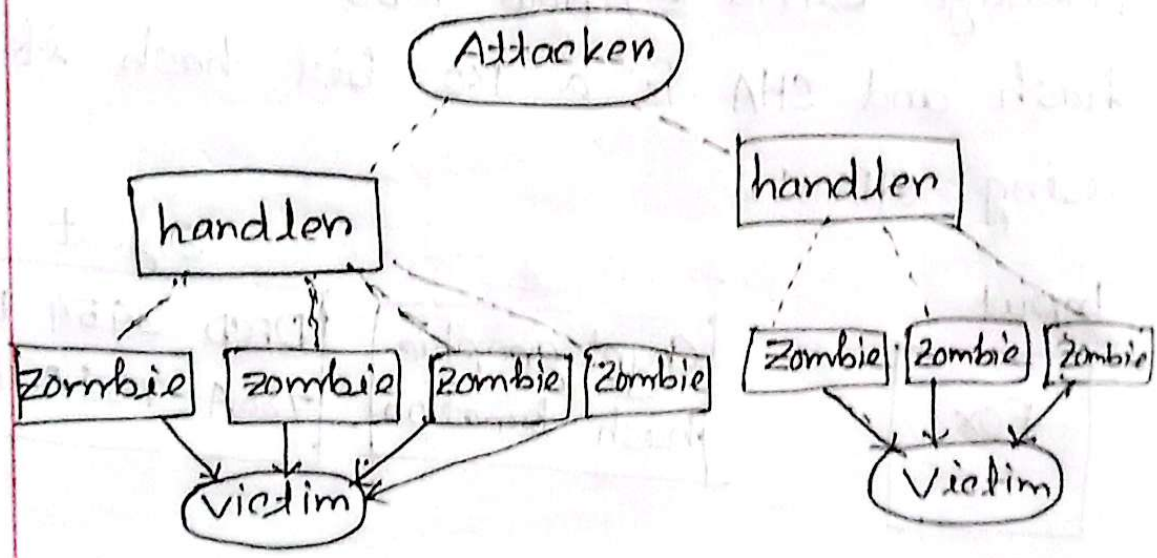
maintain data integrity. To check if our data has been modified or not, we make a use of hash function. we have two common types : SHA (Secure Hash Algorithm) and MD5 (Message Direct 5). Now MD5 is a 128-bit hash and SHA is a 160-bit hash if we're using SHA-1.



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 the network make regular upgrades, have a hardware plan for fail-over and prevent bottlenecks

in a network. Attack such as DOS or DDOS may render a network unavailable as the resources of the network get exhausted.



2. Symmetric key Encryption:

Symmetric key encryption is a type of encryption where the same key is used to both encrypt and decrypt the data.

How it works:

1. The sender encrypts the message using a secret key.

2. The encrypted message (ciphertext) is sent to the receiver

3. The receiver uses the same secret key to decrypt the message back to its original form.

Asymmetric key Enkryption :

Asymmetric key encryption that uses two different keys a public key & a private key.

How it works :

1. The public key is shared with everyone.

2. The private key is kept secret by the owner.

3. If someone encrypts a message with the public key. Only the matching private key

can decrypt it.

Types of cyber attack

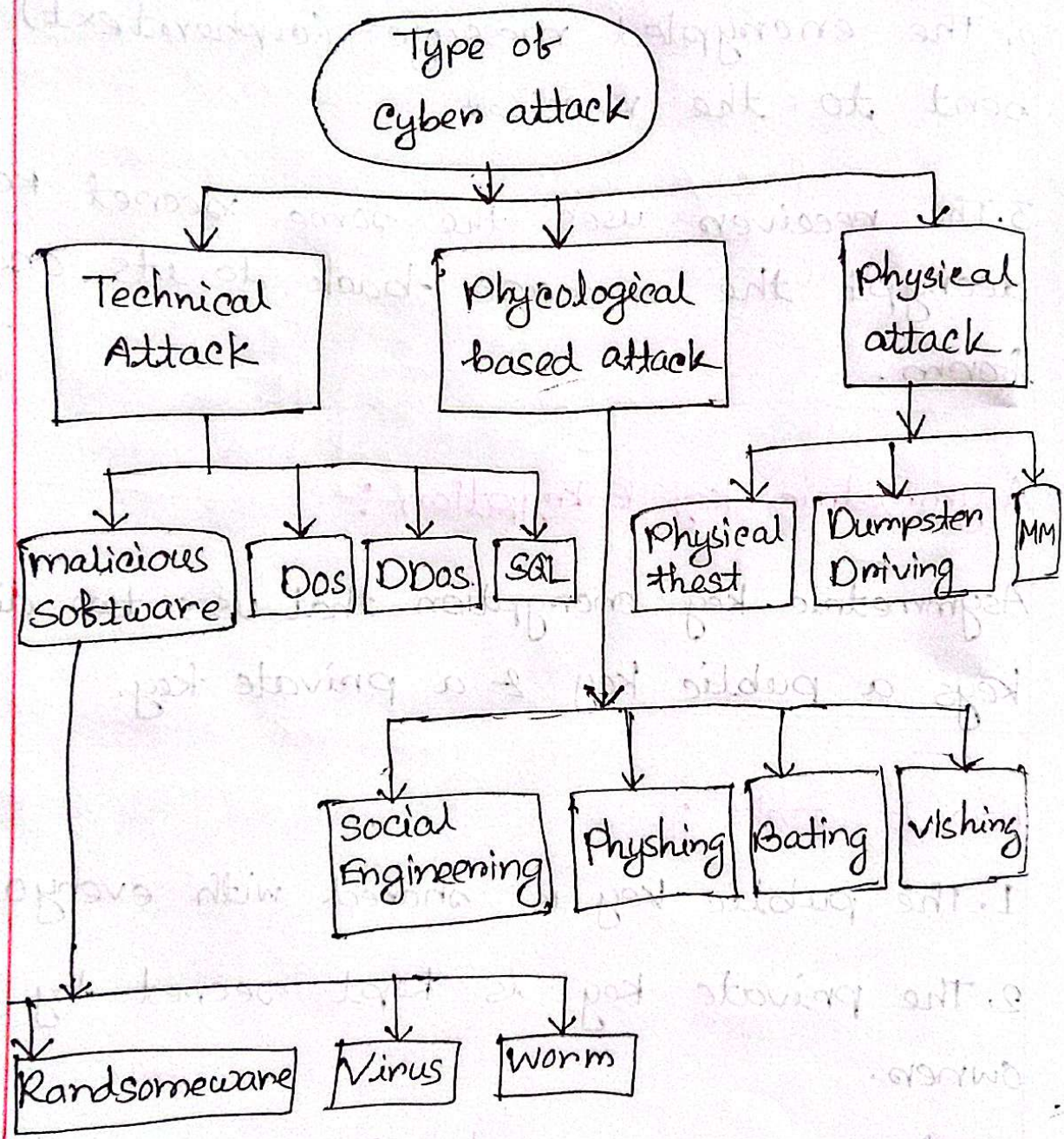


Figure : Types of cyber Attack.

1. Malware
2. phishing
3. Denial of services (Dos/Distributed Dos/DDos)
4. Man in the Middle Attack (MitM)
5. SQL injection
6. zero-day - Explot
7. Brute force Attack
8. Cross site Scripting (XSS)
9. Randsomware

Steganography :-

steganography is the practice of hiding secret information within an ordinary, non-secret file or message to avoid detection.

How it works :

A secret message is embedded inside other file using special techniques.