Introduction

* Define Information Security and Explain CIA Tried.

=) Information is a set of data which is unorganized and row form of data.

Information Security is a set of policies or principles that can use to protecting information from unauthorized system.

=) CIA Tried:

The CIA Tried is a One type of Security model that can be provide information policies For a specific an Onganization or Company.

This Model is provides guidance to every Company for the define Information Security.

CIA Tried includes this three part.

C - Confidentiality
I - Integrity
A - Availability

Page No.
Date :

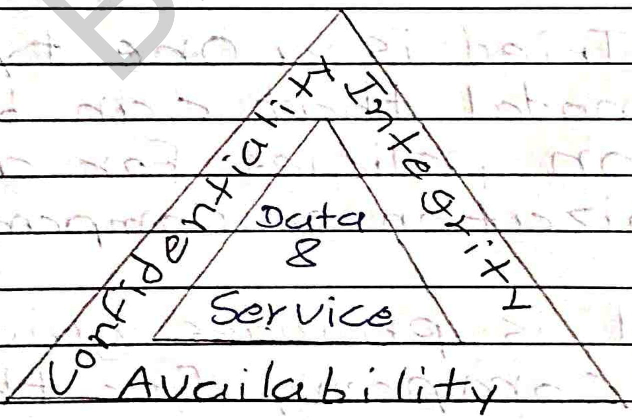
(i) Confidentiality :

Confidentiality is used to protect the sensitive information from the unauthorized system.

Information must be provided only to the authorized users or system.

In Confidentiality, we have to use Data Confidentiality and Privacy for the protect the information.

Data Confidentiality assures that only authorized system can access the information and information is disclosed for every unauthorized system.



(ii) Integrity :

Integrity is used to ensures that every information is accurate, consistent and trust worthy.

Authorized user is always get unaltered and reliable information.

Integrity can be use Data Integrity and System Integrity.

Data Integrity assures that every information can be changed or altered by only authorized user.

System Integrity assures that every function in system is performs in an unimparied way.

(iii) Availability:

Availability assures that a system must be provide information when it is needed.

Information is always accesible to every authorized system even system facing failures.

Information or Service is always work with the authorized users or system.

✱ Explain Security Goals in Information Security.

=> This are the main Security Goals.

1 Information is always protect From being sttolen, attacked or altered.

2 Information can be follow this three goals.

- Protect the Confidentiality of the Information.
- Preserve the Integrity of the Information.
- Information ~~no~~ must be available to authorized users.

3 For Protect the information we have to use CIA Tried.

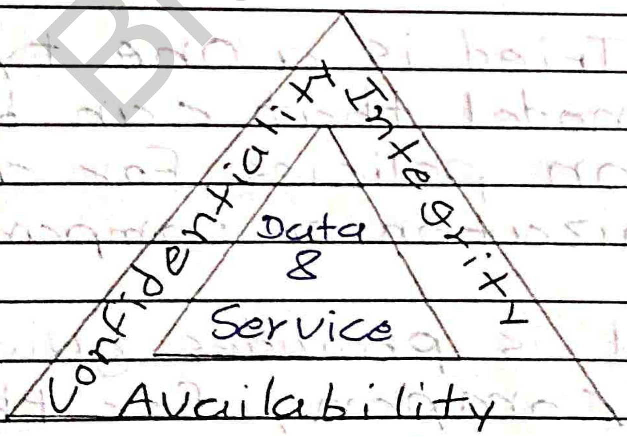
(i) Confidentiality :

Confidentiality is used to protect the sensitive information from the unauthorized system.

Information must be provided only to the authorized users or system.

In Confidentiality, We have to use Data Confidentiality and Privacy for the protect the information.

Data Confidentiality assures that only authorized system can access the information and information is disclosed for every unauthorized system.



(ii) Integrity :

Integrity is used to ensures that every information is accurate, consistent and trust worthy.

Authorized user is always get unaltered and reliable information.

Integrity can be use Data Integrity and System Integrity.

Data Integrity assures that every information can be changed or altered by only authorized user.

System Integrity assures that every function in system is performs in an unimparied way.

(iii) Availability:

Availability assures that a system must be provide information when it is needed.

Information is always accesible to every authorized system even system facing failures.

Information or Service is always work with the authorized users or system.

4 Authenticity : For access the information we have to verify the identity of users, systems and Prevent unauthorized access.

5 Accountability : In Information Security, we have to trace the actions of individuals or systems to be access specific entity.

* Explain Vulnerabilities with its types.

=> Vulnerabilities is refer to weaknesses or flaws in system that gives opportunity to attackers to access the system.

Vulnerabilities is one type of system weaknesses that can be use by threats actors.

Using System Vulnerabilities, attacker can access the authorized system in unauthorized way.

All the available system have different types of vulnerabilities even through the technologies are improving.

Date :

There are mainly Four type of Vulnerabilites.

(a) Hardware Vulnerabilites
(b) Software Vulnerabilites
(c) Network Vulnerabilites
(d) Procedural Vulnerabilites

a Hardware Vulnerabilites :

Hardware Vulnerabilites is a weaknesses of a any hardware devices in computer.

This Vulnerabilites use hardware devices system for attack.

Ex. Older Versions of System,
Hardware Misconfigurations,
Unprotected Storage device etc.

b Software Vulnerabilites :

Software Vulnerabilites is weaknesses in Software application or Operating System.

This Vulnerabilites can be accuress in the Software of a system.

Ex. Coding Errors, Insecure Configurations, Unverified Uploads etc.

c Network Vulnerability :

This is weakness of network infrastructure that can be also create using the software application or Hardware devices.

Ex. Unsecured wireless Networks, Unprotected communications.

d Procedural Vulnerability :

Procedural Vulnerability can be accuress when Organization Operational model is not protect.

IF Structure of Organization is not proper then this Vulnerability is Create.

Ex. Authentications Mechanisms, Weak Guessable Passwords etc.

* Explain OSI Security Architecture.

=> OSI stands for Open System Interconnection which is provide by ISO.

OSI also known as X.800 which is defines the systematic approach for providing the security at each layer.

OSI Provides framework for understanding and implementing security in network system.

This standard defines a set of Security Services, Security Mechanisms for seven OSI Layer.

There are three main part of OSI Security Architecture.

(i) Security Attack
(ii) Security Mechanism
(iii) Security Services.

(* Explain Security Attack, mechanism and services in short introduction.)

* Explain Security Attack in OSI Model.

=> Security Attack is one of the most important part of the OSI Security Architecture.

Security Attack refers to any Unauthorized or malicious attempt to disrupt the computer system.

There are Two Types of Security Attack.

(i) Active Attack
(ii) Passive Attack

(i) Active Attack :

Active Attack is a type of securit attack in which the attacker modified the data and send to the system.

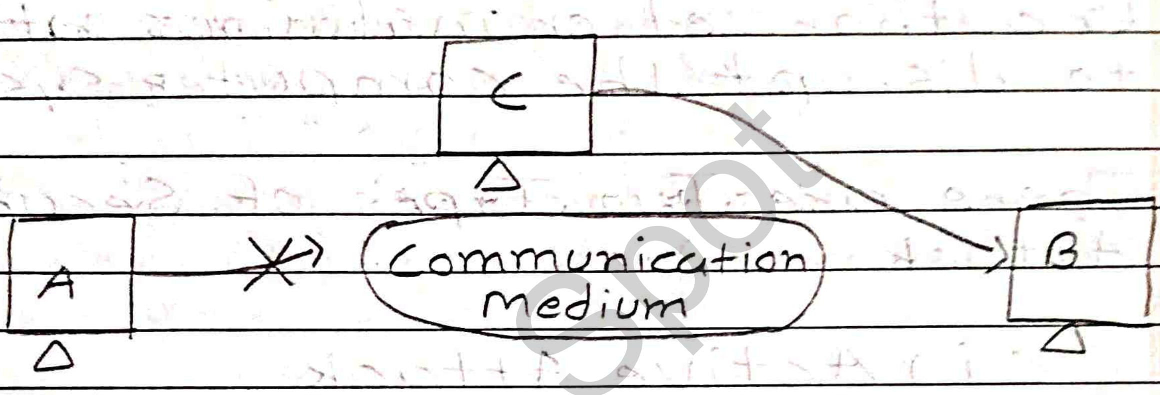
Attacker can transmits the data between two system.

Those modified data are sent to the system, that system does not known the data is changned.

This are the Types of Active Attack.

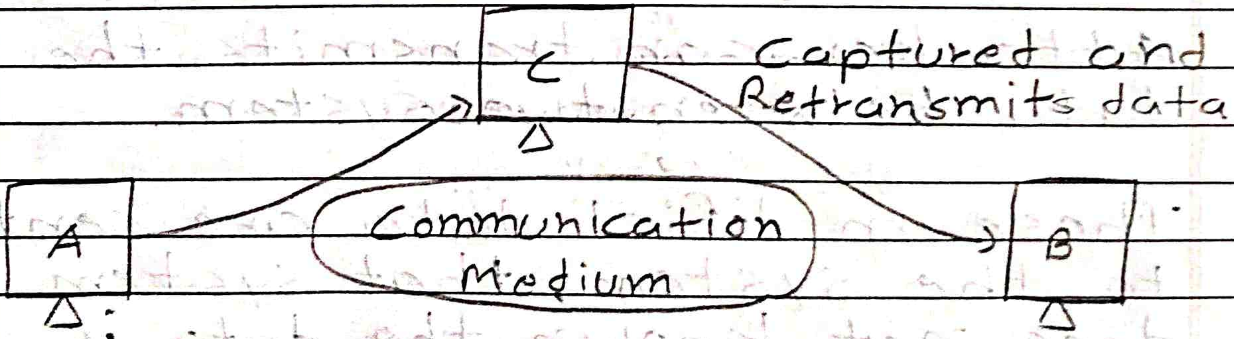
(a) Masquerade :

This is type of active attack in which one system pretents to be a different system.



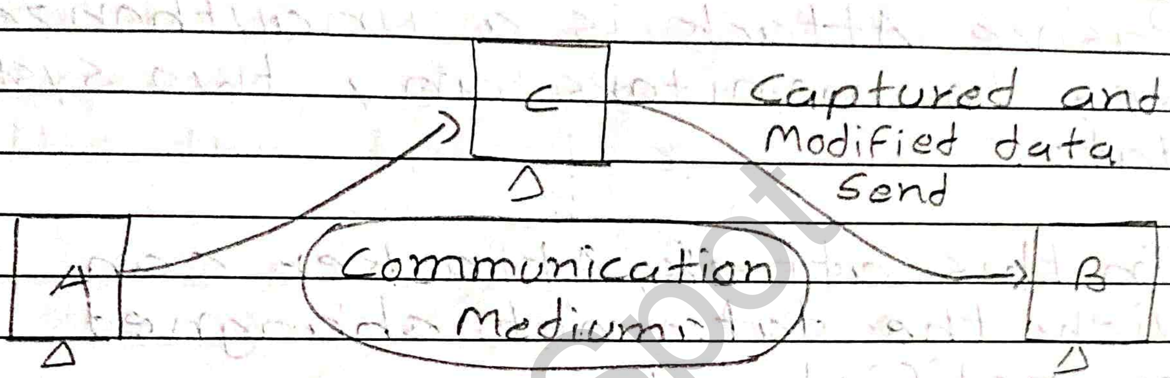
(b) Replay Attack :

In this Attack, Attacker can captured the data from the sender system and later retransmits the captured data to the target system.



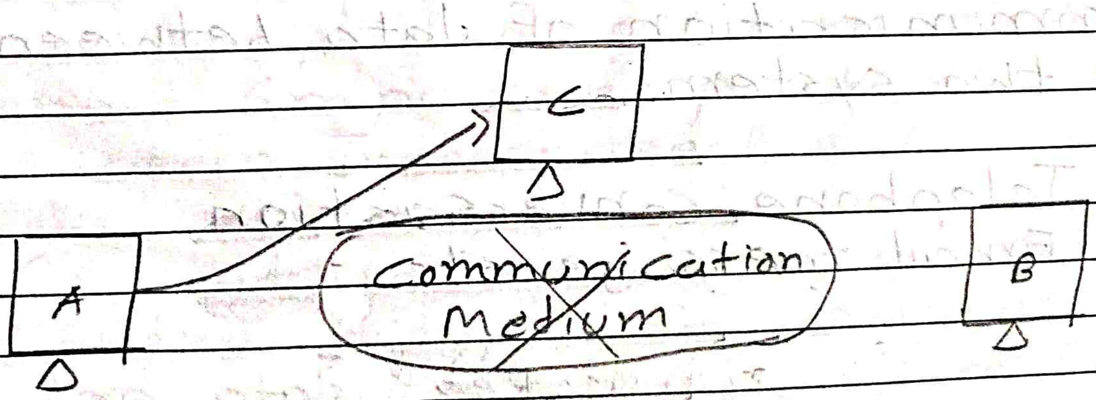
(c) Modification :

In this attack, Attacker can capture the data from the sender system, after that attacker modified that data and send to the targeted system.



(d) Denial of Services:

A Denial of Service attack is malicious attempt in which resource temporarily unavailable to users or system.



(ii) Pasive Attack :

Pasive Attack is a type of security attack in which attacker is monitors the two system communication data.

Pasive Attack is a unauthorized way to monitors any two system data.

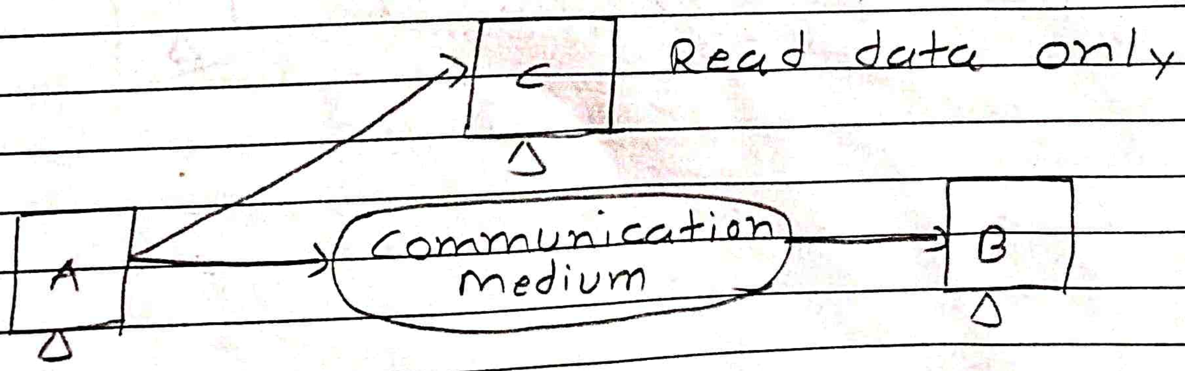
In this attack, Attacker can view the data not changned or modified.

There are Two Type of Pasive attack.

(i) Release of Message Content :

In this attacker, can read the communication of data between the two system.

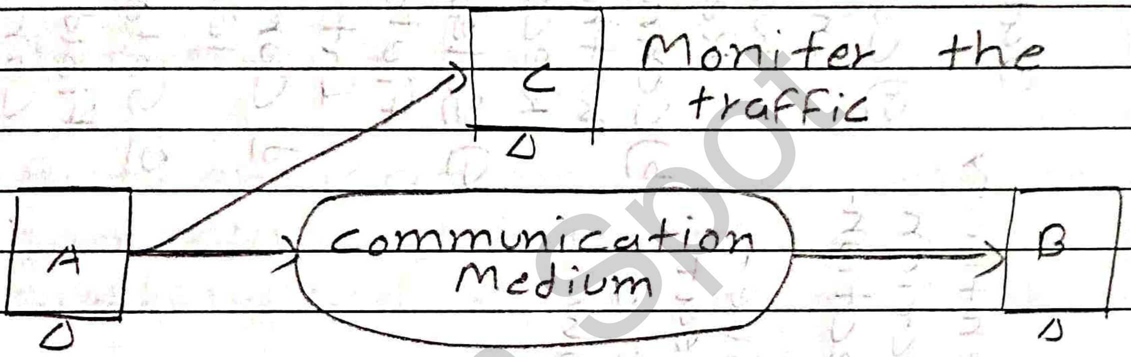
Ex. Telephone conversaction,
Email message etc.



(ii) Traffic Analysis:

In this attack, attacker is moniter the Traffic of the two system.

In this attack, attacker is moniter the length of data, Frquency of data and also identify the two hosts.



* Explain Security Services in OSI Architecture.

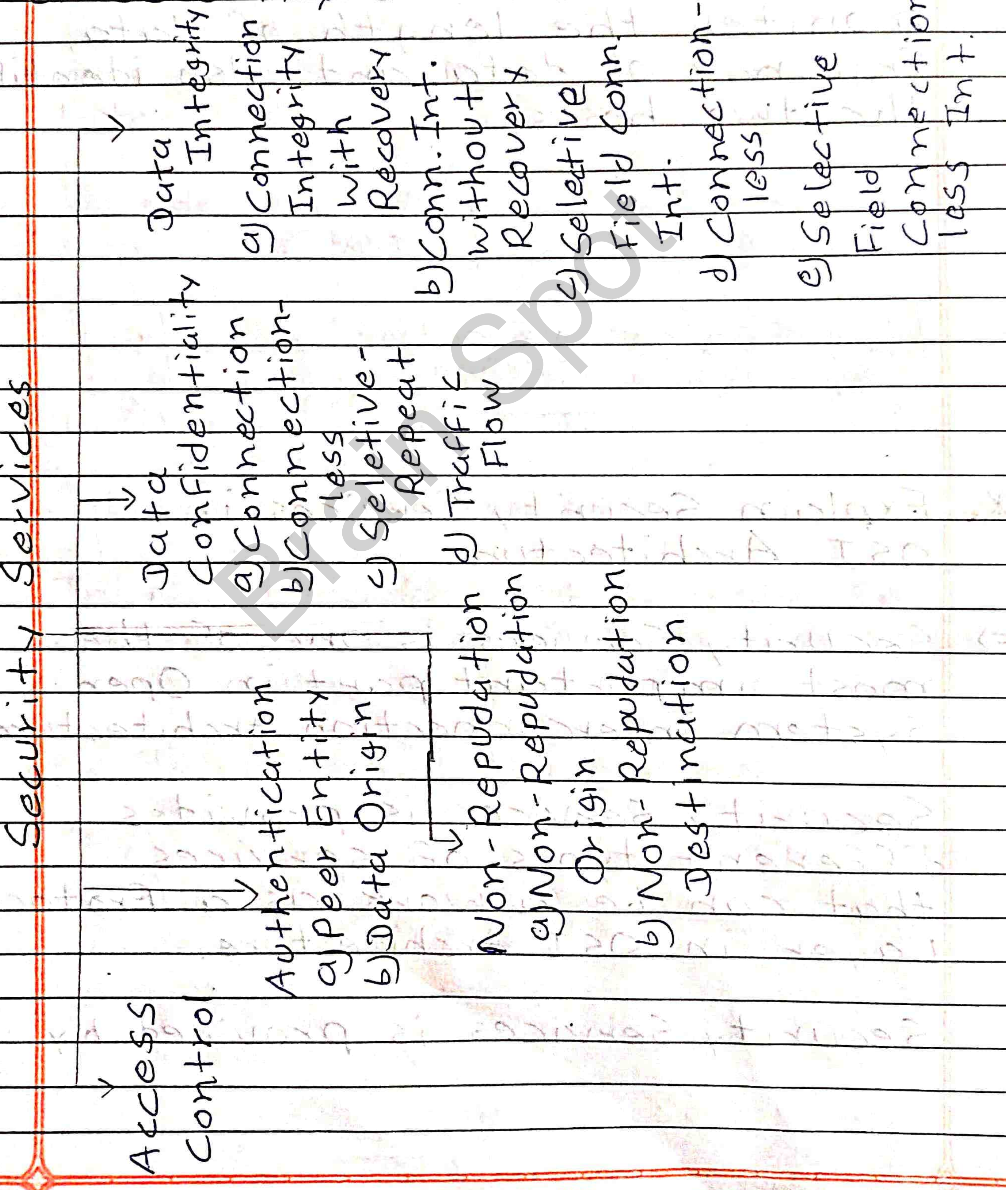
=> Security Services is one of the most important part in Open System Interconnection Architecture.

Security Services is provides different types of services that can be ~~a~~ work as a Protocol Layer in OSI Architecture.

Security Services is provided by

a system to given a specific kind of protection to system resources.

There are mainly Five Categories of Security Services.



Security Services

- Access Control
- Authentication
  - a) Peer Entity
  - b) Data Origin
- Non-Repudiation
  - a) Non-Repudation Origin
  - b) Non-Repudation Destination
- Data Confidentiality
  - a) Connection
  - b) Connection-less
  - c) Seletive-Repeat
  - d) Traffic Flow
- Data Integrity
  - a) Connection Integrity with Recovery
  - b) Conn. Int. without Recovery
  - c) Seletive Field Conn. Int.
  - d) Connection-less
  - e) Selective Field Connection-less Int.

1 Access Control:

This Services is use to protect the System resource from the unauthorized system.

Access Control only allow the authorized system to access the system resource.

2 Authentication:

Authentication is assures that communicating entity is authorized system or user.

(a) Peer Entity Authentication:

This Security Service that Verifies the identity of two system which both system do communication with each other.

(b) Data Origin:

This Security Services supports for the validation of the source of message that can send by Sender to the Receiver.

3 Non-Repudation :

This Service provides protection against the denial of any System for communication.

(a) Non-Repudation Origin:

This Service Assures that the message is send by the authorized system.

(b) Non-Repudation Destination:

This Service Assures that the message is receive by the authorized System.

4 Data Confidentiality:

Data Confidentiality is used to protect the sensitive information from the unauthorized system.

(a) Connection Confidentiality:

This Service Provides Protection of all the system User data on a connection.

(b) Connection-less Confidentiality:

This Service Provides Protection

of the system user data in a single data block.

(c) Selective-Field :

The Data Confidentiality of selective Field is provide within the user data on a connection or in single data block.

(d) Traffic-Flow :

This Services is provides protection in the information which is observation by traffic Flow.

5 Data Integrity :

This Security Service Assures that which data is ~~receied~~ received by a system that data is send by authorized system.

(a) Connection Integrity with Recovery :

This Security Service detects the any modification of any data within a entire data sequence with its recovery.

(b) Connection Integrity Without Recovery :

This Security Services detects the any modification of data within a entire data sequence, but it is not provides its data recovery.

(c) ~~Selective Field Communication~~

(c) Selective Field Connection Integrity:

This Security Services detects the any modification of data only within a selected user data Fields.

(d) Connection-Less :

This Security Services Provides the integrity of a single connection less data block and may detect the data modification.

(e) Selective Field Connection-less Integrity.

This Security Services detects the any modification of data within a selected user data Fields in Single connection less data block.

* Write the Mechanism of Services in OSI Architecture.

=> The Security Mechanism is most important Part of Open System Interconnection Architecture.

Security Mechanism is used to detect the Security attack and provide preventation of attack.

There are two type of Security Mechanism.

Security Mechanism

Specefic Security Mechanism

Pervasive Security Mechanism

a) Encipherment
b) Digital Signatuer
c) Access Control
d) Data Integrity
e) Authentication Exchange
f) Traffic Padding
g) Routing Control
h) Notarization

a) Trusted Functionality
b) Security Label
c) Event Detection
d) Security Audit Trial
e) Security Recovery.

=> Specefic Security Mechanism:

a Encipherment:

This Mechanism use the mathematical algorithm to transform data into a form that is not security intelligible.

b Digital Signature:

Digital Signature is created using private key or a cryptographic transformation which is ensure the integrity and authenticity of data unit.

c Access Control:

This Service Mechanism is use to protect the system resources from the unauthorized system which allows only authorized system to access the resources.

d Data Integrity:

It is used to assures that which data is received by a system that data is send by authorized system.

e Authentication Exchange:

The Security Mechanism ensure the identity of system using the exchange of system information.

F Traffic Padding:

In this, we have to add extra bits into a gaps in a data stream to fustrate traffic analysis attempts.

g Routing Control:

Enables selection of particular physically source routes for the certain data.

h Notarization:

This Security Mechanism Use the trusted thid party for the discusse certain properties of the Data exchange.

=> Pervasive Security Mechanism:

a Trusted Functionality:

This is process in which some

data is recognized in the correct way. like Security Policy.

b Security Label:

In this Mechanism, we have to mark the constrained to a data that define the security nature of the data.

c Event Detection:

This Mechanism is used to detect the Security - Relevant events like DOS etc.

d Security Audit Trail:

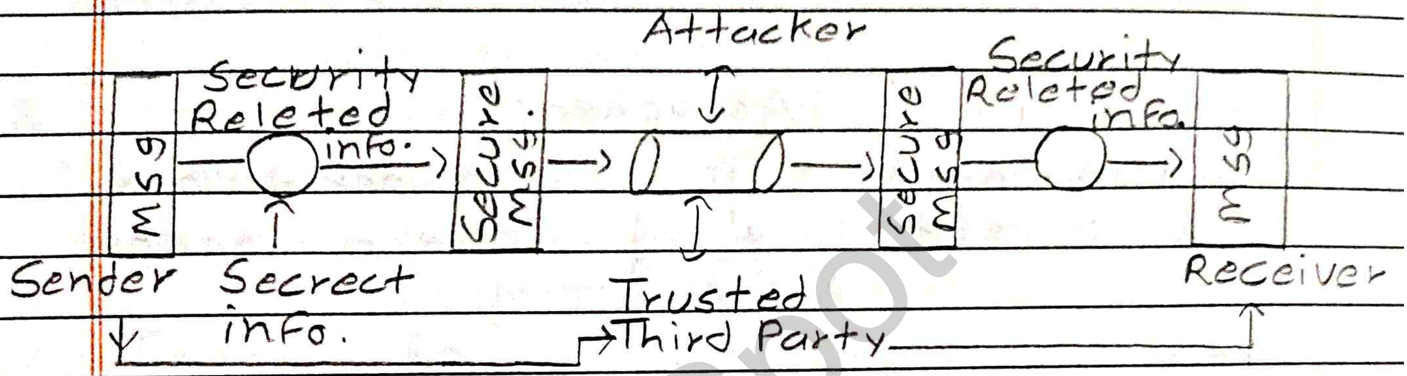
In this security Mechanism, we have to collecte the all the data and after that we have to review and examination ~~id~~ independently.

e Security Recovery:

This Mechanism is negotite with requests for event managing, and takes Security Recovery Product.

* Explain Network Security Model.

=> Network Security Model is used to describe the flow of Sending and Receiving the information between Sender and Receiver.



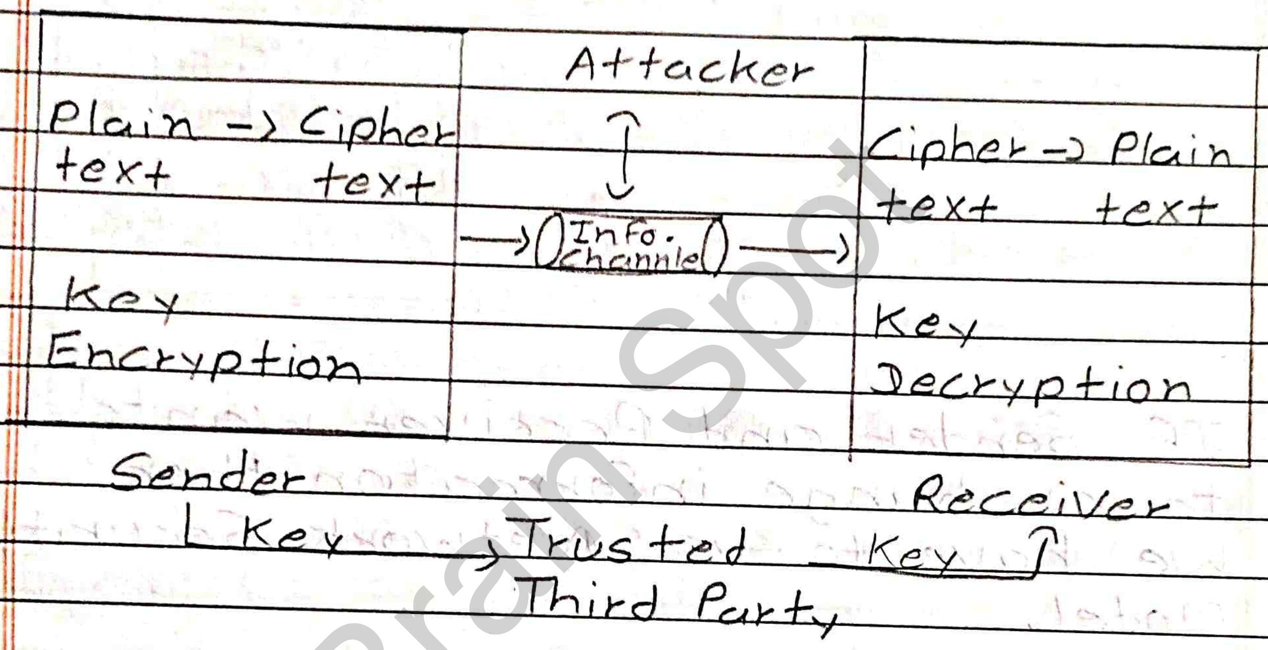
If Sender and Receiver wants to exchange information then we have to use Network Security Model.

The sender is send the all the information to the Receiver

But Sender can not send the all the information in readable from using Information channle.

If Sender send the readable form information then this information being attack by the attacker

Before Sending the information Sender have to convert this information in unreadable form, Using secret information in Information channle.



Using Trusted Third Party, we have to send the Secret Information To the Receiver.

After that, Using Secret Information Receiver convert the Unreadable information to Readable form.

Receiver is receive the Original information which is send by the sender.

=> Four Task For Designing the this Model.

1 To Transform a ~~Un~~readable data into an unreadable data Form; we have to use appropriate algorithm should be designed.

2 Model Designer need to know about the generation of the secret information which is known as key.

3 Trusted Third Party will distribute the Secret information between Sender and Receiver.

4 It is also taken care that the communication protocol that are used For Communicating with each other.