Chapter - 2
OVERVIEW OF NETWORKING, THREATS AND SECURITY MEASURES

2.1 Definition of Computer Networks

A computer is an elementary requirement of any organization. Computer is used as stand-alone machine to satisfy their necessity. With that interconnection of computers is also required for communication. Users have a preference to access information from their place only without going anywhere. This is possible only if computers are connected to each other.

The technology that connects computers to each other via communication line is called as networking. An interconnection of computers is called as a network. In short, network means connection of more than one computer to each other through communication line.

2.2 History of Networks

In the 1960s the Advanced Research Projects Agency was started funding the design of the Advanced Study Project Agency Network for the US Division of the Defense. Growth of the network began in 1969, based on strategies developed during the 1960s. The ARPANET evolved into the modern Internet. In 1969 the four nodes were connected together to form the network.
2.3 Networking Concepts

These days’ computers are used at nearly every place such as offices, shops, in various institutions etc. With the growth in technology, these computer networks form the core of communication. Network can be well-defined as a collection of autonomous computers and associated devices connected together by communication channels like cables or telephone lines etc. In the network, the computers work as standalone machines but can communicate with other computers as and when required.

Connection of two computers allows sharing of data. In a network, one computer drives the data and second receives the data. The computer who sends the data is transmitter and other second called as a receiver. Data is transferred from end to another end by the communication line.

![Communication Channel Diagram](image)

Figure 2.1: Basic Concept of communication
Networks have three assets.

Procedure: This controls the information communication.

Structural design: The design includes the physical structure and functionalities of the network. The role of computer is very important in the network architecture.

Topology: The geometrical arrangement of resources, remote devices and communication facilities is known as network topology or network structure. A network topology determines which element in a computer network can communicate with each other.

2.4 Need of Network

Network does not only provide software sharing but also hardware sharing is also possible. In any small institute, it has computers, one fast printer and a large capacity disk then networking makes it possible for all computers to share a printer and storage disk. So it reduces network cost.

Stand-alone computer are used for processing. But keeping a large quantity of data on a single computer is not possible. In that situation it would be necessary that multiple devices are used together to store data. P1, P2 and P3 are three computers, sharing single common storage device. It helps to share more data. It increases the processing speed, as a data is processed by multiple computers at the same time.
Some information centers store large informative data which is well organized. User may recover the information or data from his/her place. But it is required to connect the computer with communication centers.

This means the important use of the networking is to share files or data and to increase the processing speed.

Sometimes networking is necessary as a single computer is not able to fulfill a task of the organization and in this case network helps to complete our requirements. As a result networking becomes the basic requirement of any organization.

2.5 Network Types

There are two possible ways to build a network depending on the communication method.

1. Point-to-point network

In this type data travels through source to destination in a proper channel. That means data has to travel from one to other and other to forward. Multiple routes or ways are available to transmit the data. Many components are used as intermediate
machines to transfer the data. Most point-to-point networks use cables or wires for connections. But wireless links are also useful for long distance networks.

Very primary example of point-to-point network connection is personal computer with printer. A cable is a physical link that connects computer with printer.

2. Broadcast network

This is single line connection shared by multiple devices. Data is transferred through the channel. Data consists the destination address also. Every receiver checks the endpoint address. If the address is not same then terminal ignores the signal.

Most broadcast network is used to send data to multiple receipts. If signal is sent to all terminals in the network then that is called as broadcasting. If the signal is sent to some of the terminals then that is multicasting.

2.6 Types of Network according to Communication type

The network types describe the way in which resources attached to computers can be accessed by another computer. Network can be divided in two ways according to connection type.

1. Server Based Network

2. Peer-to-Peer Network

3. Hybrid Network

1. Server Based Network

All computers are connected to the central unit. That central unit may be central computer or a device. It controls all other computer in the network. That central computer is known as a server. All other computers in the network are termed as clients. If server does all processing, then all other clients act as input and output
devices. This type of server based network is denoted as centralized network. For this server must be with high speed and high storage capacity.

![Figure 2.3 A Server Based Network](image)

**Advantages**

1. Central computer is used to manage a complete network.
2. It is suitable for large network.
3. Central data processing with possibility to distribute the computing task.
4. Security can be maintained.

**Disadvantages**

1. Special computer is dedicated as a server.
3. It is not affordable for small network.
2. Peer-to-Peer Network

All stand-alone computers are connected to each other. A special computer server is not used to control all other computers. The network, that connects every computer to every other computer, is called as peer-to-peer network. This network is also called point-to-point network.

Every computer in this network is called as peer. Each computer is independent for input, output and to store the data. Each computer acts as a server as well as a client. Every computer can share data or resources of other computers.

In this network, all P1, P2, P3, P4 and P5 are connected to each other. Pn acts as a server as well as clients. If other wants to access the data from Pn then Pn is a server. If Pn needs to access data from other then Pn is called as client.

Central controlling is not done by any of the point. This type of network is called as decentralized network. In small organization, decentralized network is suitable if computer number is less than ten. Different departments can be connected together to share data and resources. It increases storage capacity with security.

![Figure 2.4 A Peer-to-Peer Network](image-url)
**Advantages**

1. Suitable for small network.
2. No special computer is used as a server so less expensive.
3. Easy to install.
4. Flexible to configure.
5. Every computer is stand-alone machine. Every machine is treated on equal level.
6. It supports distributed processing so the increased load will not affect the system overall.

**Disadvantages**

1. Difficult to administer.
2. Shared resources are generally somewhat slower than dedicated resource.
3. Due to limitation of number of connection to one computer decentralized network is not suitable for large network.
4. It does not support centrally managed security. It does not provide the backing up of files.

To eliminate these errors or the disadvantages of the both network, user may go for the hybrid network.

**3. Hybrid network**

Hybrid network is combination of centralized and decentralized network. All clients are connected to the server. Again all clients are interconnected to each other.

It takes advantages of both the networks and helps to eliminate drawbacks of each other. Failure of central computer damages whole network. But hybrid network also works on peer-to-peer connection.

Server ‘S’ is connected to every peer (P1, P2 and P3) again P1, P2 and P3 are interconnected to each other.
User can select any type of the network depending upon the requirement.

### 2.7 Network Topology

The physical arrangement of the cables, computers and other peripheral devices to form a network is known as a topology. It is the shared communication medium that makes the backbone of the system. Computers and the other devices including the server are connected to this linear cable for communication.

Advantages- the advantages of a network with the bus topology are: it is very convenient to install. And do not require much cabling.

Disadvantages: The disadvantages of a network with bus topology are: it is tough to identify the reason if the complete network shuts down.

Star Topology: It is the most common topology used. In this all the workstations are connected to a central connection point called a hub. Any data that is sent to the other computer first goes to the central hub and from there it is redirected to the destination computer.
Advantages: are easy to install.

Disadvantage: The disadvantage of the star topology is it requires more cable length. Failures in the central hub will break down the whole network.

In the ring topology, the advantage is, it is easy to detect faults in the network.

Less number of cable wires are required. The disadvantage is if one wire breakdowns down leading to the breakdown of the entire network.

2.8 Advantages of Computer Networks

These days’ computer networks are a vital part of any organization.

*Resource Allocation*

There are some costly computer resources which cannot be provided separately to each system like laser printer, plotter, scanners etc. and also some of the computer softwares can be shared among the computers connected in the network. So, in an environment where hundreds of computers are being used, network facility saves a huge cost involved in purchasing hardware and software components for individual computers. So by using network computers can share exterior devices printers, modems and scanners etc.

*High Reliability*

This can be achieved by having the data or information available over the network on the other computers. The copy of the files can be stored on multiple machines over network and hence in the case of failure of one the machine, other machine can become the source of the information or data.
Distribution of the workload

The work can be reloaded over the network onto more than one computer in case of saturation of computer because of too much load over it.

Saving money

It is economical to set up a network of large number of small computers than to invest in large ones.

Expandability

The size of the network as well as performance of it can be expanded by adding more machines and devices to it.

File Sharing and Remote Database Access

A computer network allows sharing of files and access to remote database. You can easily access the files stored on various computers on a network. Also, networking allows many people to work simultaneously on the data stored in a database.

Ease of Communication

Computer networks allow people to communicate through emails and instant messaging facilities. This makes the transmission of information easier, more efficient and less expensive.

Protecting information

The network provides additional security for any organization’s important data in terms of login and password. Also different levels of access can be set in a network.
2.9 Disadvantages of Computer Networks

The following are the disadvantages of the computer network:

(1) If the server is down then users may not be able to use the programs and there are the chances of data loss.

(2) If the network stops operating then the computers connected to the network cannot be used, thus affecting the performance of the whole system.

(3) If users on the network increase then the performance lowers.

(4) In the wired networking or in the wireless networking threats are there for the data and the networking.

(5) As compared to wired networking there is more vulnerability in the wireless networking.

(6) Though the every learning field is using the security measures to safeguard their data and the networking but the hackers are finding their ways to get into their network and spoil their valuable data.

2.10 Types of Computer Networks based on the Geographical Area

A computer network can be as simple as two computers connected directly with each other or it could be as complex as millions of computers network depends on the particular requirements, interconnected like to connect all the computers within an office or educational institutions we need a smaller network, but for connecting the offices of an organization across the countries we need a network spread across the large geographical area. They are classified as follows:
LAN: small geographical area like an office, building or campus. All the computers in LAN are connected through cables or wireless links for communication. The number of computers in a LAN can vary from two to several hundred computers. As all the computers are located in a small geographical area, the communication speed is faster and chances of data loss are very less. Generally, its size ranges from 0 to 10 kms.

MAN it covers a metro or a city. MAN is used to connect the offices of an organization spread across the city. The medium used to connect the computers in MAN is similar to that in LAN. As it covers larger area than LAN, the cost involved in setting up a MAN is higher than LAN. Size of MAN can range from 10 to 50 kms.

WAN (Wide Area Network) This type of network covers a very large geographical area, across the country or continent. WAN is generally established by the large institutions, having workplaces spread across the country or in different countries. The medium used to connect the computers in WAN can be leased lines, fibre optic cables, radio waves or satellites. Because of large distance covered by WAN, the data transfer rate is slower and the chances of data transfer error are more as compared to LAN.
2.11 Network Hardware

To connect the computers in a network, various types of hardware components are needed depending upon the type of a network. These hardware components are:

Server

It is normally dedicated, that is it performs no other task besides the allocated task.

For example, a file server is a computer that manages storage and retrieval of files. A print server is a computer that manages one or more printers required in a network.

Workstation

A workstation is a computer intended for individual use in networking environment. It is like a personal computer except that is it is connected to other computers as well as to the main computer that is the server.

Network Interface Card (NIC)

Also known as a LAN card or Ethernet Card is the most important component used for establishing the network. It allows a computer to participate in the network. Information from the computer is transmitted through NIC connected on the motherboard.

Transmission Medium

Transmission medium carries the data signal from one computer to another.
**Hub**

A hub is central hardware device in a network that manages traffic across the network. A hub divided the bandwidth or communication speed equally among the computers connected to it.

**Switch**

A switch that manages the flow of information among the PCs and devices connected to it. The rate of flow of information is linked to the speeds backed up by the switch and the devices.

**Router**

This is a network hardware device which is used to route the data across the different parts of the network when the computers are connected in WAN.

**Connector**

A connector is used to join two computers or networks together.

**2.12 Network Software**

*Networking Operating System (NOS)*

NOS control the network by co-ordinating, enabling services and sharing of the resources among the networked computer. Some examples of NOS are: Microsoft server, Microsoft Windows Server 2008, Microsoft’s LAN Manager, Uniplexed Information and Computer Systems (UNIX), Novell NetWare.
Procedure

It is to be transferred among the computers on a network. There are various types of protocol that are used in a network.

2.13 Threats in Networks

A passive adversary attacks on all network communication, with the goal learning as much confidential information as possible.

The other is an active intruder, which will

- Modify messages at will,
- Introduce packets into the message stream, or
- Delete messages.

A. Passive Attacks

The passive attacks can occur in the following ways:

1. Eavesdropping: the unauthorized captures of transmitted data either by some form of the line trapping or form the compromising emanations broadcast by the electrical signals in the line. Radio, optical and microwave signals can be similarly intercepted secretly.

2. Traffic Analysis: Even if enciphering has protected the message, an analysis of the traffic down the line can, in many circumstances, reveal much to an outsider. The number, size, frequency and times of messages sent, their sources and their destination can indicate, for example an impending takeover bid, or the launch of a new product.

Thus a passive attack is an attack where an authorized attacker monitors or listens in on the communication between two parties.
B. Active Attacks

The aggressor is able to convey data to one or both of the parties, or block the data or information stream in one or both directions.

C. DOS Attack

Anybody with the elementary information of network safety can attack on the networking.

D. Digital Threats

Virus (Vital Information Resource Under Siege): Computer viruses are the malicious programs having the ability to replicate and execute themselves. They can attach themselves to the other program, files or data stored in the system automatically without any instructions from the user. It can enter in a computer by different means like when one copy some data from the virus infected system to another uninfected system or while downloading some programs from the Internet or it can come to system as an e-mail message. A computer virus spreads itself from one computer to another and interferences with the normal operations of a computer. Viruses attach themselves to any type of executable and system files, causing the unusual behavior of the programs or sometimes causing the system crash. Based upon their working behavior, target infection computer viruses can be categorized as below.

(i) Boot Viruses: Every time a system is booted with an infected hard disc, these viruses become active and start infecting the stored data. Danish boot, PC stone, Joshi, brain, Empire, Azusa, Michelangelo, etc. are the examples of boot viruses.
(ii) Polymorphic Virus: Polymorphic viruses are written such that it changes its code whenever it passes to another machine. Hence it is difficult for any anti-virus scanner to locate them.

(iii) Macros: The main target area of these viruses is to infect the data file of the system like MS-Word, MS-Excel files etc. These types of the viruses destroy the data stored in the system causing irrecoverable damage sometimes.

(iv) Worm: It requires human action such as transferring of an infected file to spread itself. A worm can spread without any human action too. Worms can harm to a computer network as blocking the network and reducing the speed of the network. They reduce the storage space and available memory of the system.

(v) Torjan Horse: After getting installed, it allows unauthorized access to the computer. Torjan effects are very dangerous as they allow the computer to be remotely controlled by someone else and can cause loss of the personal and confidential information. They are not self-replicating and the only way, they can spread is copying to the other system, e.g. Zeus, Beast, Back Orifice, The Blackhole Exploit Kit etc.

(vi) Stealth Virus: these types of viruses are capable of changing their appearance by changing their codes. This way, they can hide their existence from the Antivirus programs. Sometimes, it hides the increased size of the file due to virus infection causing the file to be scanned as an uninfected file. Frodo, Brain are the example of Stealth viruses.

(vii) Program Virus: It also known as the parasitic viruses, they infect the program files of the system having extensionas.com, .exe, .sys, .ovl, .dll, .Scr etc. These viruses do not affect the boot records of the system. Program files are their attractive
targets, because these files are used very frequently and moreover the format of these files is quite simple. So when these programs are used they become active in the computer’s memory and start their destruction work.

(viii) Bomb: Viruses that active on certain dates are often called time bomb. For example, Jerusalem –B or Israeli Virus or Friday 13th Virus waits for Friday the 13th and deletes the program files executed on that day.

Thus Viruses, worms and Torjan Horse may harm the data or affect the performance and the speed of the computer.

(ix) Data Theft: It is a very serious problem for computer networks. People break into computer networks to either disrupt their functioning or to steal confidential information. Hackers are the computer experts who can break into the computer systems and networks. There are two types of hackers – white hackers and black hackers. White hackers study and break into networks to find and fix security loopholes. They offer their services to almost all organizations and educational institutions to make their networks more secure. Black hackers or crackers have a criminal intention. Some examples are cracking confidential information like results of the students in any educational institutions and attacking the computer network of any organization.


2.14 Need of the Network Security

User can access the information, hardware and software by logging to the network by their ID and the password. Network security includes a variety of computer networks that are used by educational institutions, government agencies and individuals etc.

It is seen that the academic and the administrative computing systems used to be more out-of-the-way either intentionally due to the security reasons or as a result of limited interconnectivity. But today it is seen that nearly all information like administrative, personal details of the student and the teachers etc. can be obtained through a network. Course materials are presented over the network and even students are submitting their assignments. When registration, application forms, materials and the students grades are submitted and recorded over the open network better security are needed.

A significant amount of research has been done to resolve network security problem but it still remains to be a challenging due to increased difficulty and various threats peeping into the networks daily. A lot of techniques like firewalls, verification, anti-virus softwares etc. are being adopted but they are not result into a complete solution. As a result these tools and techniques proposed earlier may become out-of-date for solving network security problems at large. Hence it becomes the responsibility of the network managers to work more on these techniques to obtain the secure network environment.

Network security is very important issue for any institute. Due to the fast network growth the security threats are also exploring day by day which affect all network applications and even the internet services. As the institutions are growing day by
day it becomes the first priority of the network administrators to secure the data and the entire network. This paper describes the significant measures and factors needed for developing a secure network.

In the present situation wired and wireless networks are commonly used in educational organizations to meet the various requirements of education institutions. Due to the increase in the network in the educational institutions new sorts of security threats and vulnerabilities are also increasing, making wired and wireless networks uncertain and unreliable. In this research paper, a study of various types of security threats and security techniques in educational environment and ways to neutralize them has been discussed.

Educational software systems have a progressively an important existence in learning process. Hence almost every institution are using the network to improve the teaching and learning process. Network security is key question of the new generation of computing because various types of attacks are growing day by day. Creating a network is not a big subject for network administrators but protecting the entire network against the different types of attacks is a great issue. There are various methods and tools are available nowadays for destroying the entire network. This paper mainly emphasizes on the network security measures and also some main issues that can affect entire network.

The need for networking is demand of the today’s world. This paper gives the complete details of the advantages of the networking and different forms of the networking and why there is the requirement of security measures in the networking. The need of the various network security measures to safe the information from the network attacks. Researcher has made the efforts to find out the cause that even though the security measures are used still important data and
information are getting hacked and misused by the hackers. So it is the time that each organization should start working more on how to minimize the risks factors.

Academic organizations are among the most targeted information systems in the world. Their extremely decentralized set-up makes it difficult to safeguard reliable security measures across their networks. Furthermore academic institutes have different departments with various users like faculty, staff members, learners, and scholars etc. who are accessing data from the network. The possibility and impact of threats and damage to the privacy, integrity and availability of the data have been higher. The educational institutes are aware that the security of their information assets like IT infrastructure, confidential records, faculty and students personal details etc. is their uppermost priority in terms of risk and even institutions stability and reputation. Very minute research work has been carried out in this field. This paper suggest to work more on the implementation of the Information Security System in academic institutes and make the system and network secure against the unauthorized users.

Network security is intertwined in all the types of organizations, enterprises etc. Here more focused is done on the educational institutions as vital information regarding the institution, student’s personal details, results etc. are saved on the network. Hence it becomes essential to secure our data against the network attacks.

Safekeeping has to be connected with: security, stability and dependability. So to implement the secure network model first look to the policies and requirement of the organisation and the second step is to see the cost to design the network structure. This paper even helps the network managers and the software companies to work more on the network security measures so that they can give the fully secured environment to the every organisation. Hence we can say that security is
everyone’s requirement and only with everyone's support, a smart strategy, and steady practices it will be attainable.

**2.15 Security threats**

There are various ways and means in which threats can be given to the security. Generally the two main levels in which threats can be given to the system are:

- **Inside attack**: Studies have shown that 70% of the attacks come from someone within the organization or someone with inside information. This is because the insider has complete knowledge of the system’s functioning.

- **Attacks from outsiders**: The outsiders who would attack the security may be either a competitors desperately needing the sensitive internal information of any of the organization or just making fun or trying out their lick or experimenting by disturbing the systems without any special reasons.

In general the means of the threats to the system security are found as:

1. Threat to Availability: information is not available whenever demanded.
2. Threat to Integrity: someone has deliberately tampered the information.
3. Threat to Confidentiality: information illegally accessed by someone.
4. Threat to Authentication: valid user identity is penetrated.

- **Cookies**: Suppose that the client sends as HTTP request. The web server locates that page on its disk sends it back to the client and completely forgets about this interaction. If the client wants to continue this interaction it must identify itself to the server in the next HTTP request. Otherwise the server would not know that this same client and sent an HTTP request earlier. Since there are number of interactions between the client and the server, there must be some mechanism
for the client to identify itself to the server each time it sends a HTTP request. For this cookies are used. They are a popular mechanism of maintaining the state information i.e. identifying a client to a server. Cookies are just one or more pieces of information stored as text strings in a text file on the disk of the client computer.

These attacks take two main forms:

(a) Packet Sniffing (also called as snooping)

(b) Packet Spoofing

Since the protocol used in this communication is called as Internet protocol (IP), other names for these two attacks are (a) IP sniffing and (b) IP spoofing. The meaning remains the similar.

(a) **Packet Sniffing:** Packet Sniffing is a passive attack on an ongoing discussion. An attacker need not capture a conversation but instead can simply observe that is sniff packets as they pass by. To stop an attacker from sniffing packets, the information or data that is passing needs to be protected in some ways.

This can be done at two levels:

(i) The data that is travelling can be encoded in some ways.

(ii) The transmission connection itself can be encoded.

(b) **Packet Spoofing:** In this method the receiver the containing a false address would unintentionally send replies back to the forged address called as spoofed address and not to the attacker.

This can be lead to three cases:

(i) The invader is between the destination and the forged source; the attacker can see the reply and use that information for hijacking attacks.
(ii) The attacker need not see the response: if the attacker’s purpose was Denial of Service (DOS) attack, the attacker need not bother about the reply.

(iii) The attacker does not want the reply: the attacker could only be angry with the host. So it may place that host’s address as the forged source address and send the packet to the destination. The attacker does not want the reply from the destination as it wants the host with the forged address to receive it and get confused.

(c) Sniffer Attack:

Using a sniffer, an attacker can

- Study our network and cause our network to crack or to become corrupted.
- Read our communications.

2.16 Various Security Models

There is various security models are possible within the organization to act as the network security model. But the models are limited to certain basic methods.

1. No Security: This is the basic model of security with which the general security mechanism will begin. This model implies that the system is separated from the network and the internet. The system may be used only for the internal vertical applications with which only data entry is taking place and no other external devices are used. In this case of situation the user can decide not to have any security measures. Thus it is highly risky.

2. Security through obscurity: This model keeps the security hidden, which cannot survive for a long time. This system will implement the security measures without revealing its details to the user. This may lead to the problems related to
the misunderstanding about the security process by the user or misuse by the attacker.

3. Host Security: This allows the security measures to be enforced individually in each and every host. This is simple and safer method to implement. But this will not cover the diversity problems. The individual systems may be having different structures and with different security models. This will do well as long as the systems are working individually. This method will applicable for the standalone machines or the individual horizontal users. This can also be used within the network where the security concerns will be implemented in the individual user levels, which will be more reliable and application specific. But this will create problem when it is connected into a network and the communication boundary enhances.

4. Network Security: This method will be implemented when the boundary of the network increases and the organization boundary is expanded with various business processes. This includes the method which is more complicated but more transparent and secured comparing to the earlier models.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>No Security</th>
<th>Security Through Obscurity</th>
<th>Host security</th>
<th>Network security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>Highest</td>
<td>High</td>
<td>Medium</td>
<td>Less</td>
</tr>
<tr>
<td>Scalability</td>
<td>NA</td>
<td>Low</td>
<td>Less</td>
<td>High</td>
</tr>
<tr>
<td>Cost</td>
<td>NA</td>
<td>Costly</td>
<td>Moderate Cost</td>
<td>Less cost</td>
</tr>
<tr>
<td>Efficiency</td>
<td>NA</td>
<td>Less</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>
2.17 Networking Security Models

As the threats are increasing in the data and the network security the network security measures are essential to use. These tools are encryption, authentication, intrusion-detection, firewalls etc. Cryptographic, firewalls, intrusion detection, antivirus, passwords and algorithms are some of the security models to safeguard our data against the illegal accessing.

Some of them are explained below. To avoid the threats in the network various network security measures are given below:

(1) Firewalls

(2) Antivirus Software

(3) Passwords

(4) Cryptography

(5) Algorithms etc.

(1) Firewall

A firewall is a software program or hardware that stops the hackers, viruses and worms that try to reach the computer. Firewall scans every message and blocks that information that does not meet the security norms. The firewall itself must be tough enough, so as to reduce attacks.

The primary benefits of using a firewall are:

(1) Shield from Vulnerable Services

(2) Logging and Statistics on Network Usage, and misuse of it.

(3) Policy Enforcement
**Advantages of Firewall**

1. It enforces a security policy by allowing a single point for implementing and controlling all security decisions to be made.
2. It filters monitors and logs the sessions between any two networks. As a result, our exposure to the internet is also limited.

**(2) Authentication**

Features of the authentication are –

- User identification and password.
- A signed digital certificate or even a fingerprint.
- User’s voice, hand configuration, a fingerprint etc.

**(3) Intrusion Detection System**

IDS are mainly concentrated on recognizing possible occurrences, logging information and reporting attempts.

**(4) Antivirus software**

Anti-virus softwares are used to protect a computer from all types of malware. Antivirus software can detect viruses; worms etc. and warn the presence in the computer. It can deactivate the malware and clean the computer of different types of the malicious software.

Antivirus softwares are the utilities which prevent the viruses to enter in our system. They can also detect and remove the virus entered in our system. There are the memory resident programs and get activated as soon as the system is started. It checks all the files in the system and if any virus is detected, it removes the virus. Also while working on the computer if some infected storage device is found, it generates the warning message and stops the data transfer.
It is an application program which is designed to detect and remove viruses, worms and Torjan horses from the computer system. Anti-virus software looks for these computer threats in all the files and folders of the computer system. It looks for changes and activities in the systems that are typical in case of virus attack. Scanners that are built within the anti-virus software look for particular types of codes within programs. If a virus is detected the anti-virus tries to remove it from the system. The most popular anti-virus softwares are Norton antivirus and quick heal total security.

Install antivirus packages. Packages like K7 ultimate PC security, Norton Antivirus, Kaspersky Antivirus, Panda Cloud Antivirus, Quick Heal Antivirus, AVG, Avast, McAfee, PC-cillin etc. are far better at blocking malware than at cleaning them out. They also provide regular updates that can be easily shared throughout a network.

(5) Cryptography

The term Cryptography means the concept of encryption and decryption together. Cryptography is the method in which the plain text message is encoded that is called cipher text at the transmitter’s end, which is then conveyed to the receiver. The receiver then decrypts to get the original message back.

Cryptography is also termed as an art or method to achieve protected communication between the communicating parties by encoding the message between them such that no third party can gain anything useful out of interception.

Various techniques are utilized for this purpose of cryptography. Broadly these techniques fall into two categories.
(1) Symmetric key Cryptography: In this the significant component used is the equal for the both encoding and decoding.

(2) Asymmetric key Cryptography: In this the key element used is unlike for both encryption as well as decryption.

Thus this chapter explains about the various types of networking depending upon the geographical area, various threats which are associated with the networking and the data and the various security measures which helps the educational fields and even the other organisation to protect their data from the unauthorized users.