Computer Security:

Definition: Computer Security refers to the protection given to computers and the information contained in them from unauthorized access. The practice of computer security also includes policies, procedures, hardware and software tools that are necessary to protect the computer system and the information processed, the measures and controls that ensure **confidentially**, **integrity** and **availability** of the information.

Confidentially: Confidentially ensures the information is available only to those persons who are authorized to access it. Strict controls must be implemented to ensure that only those persons who need access to certain information have that access. The most common form of access control is the use of passwords.

Integrity: - Integrity ensures that information can not be modified in unexpected ways, as loss of Integrity could result from human error, international tempering, or even catastrophic events.

Availability: - Availability prevents resources from being deleted or becoming inaccessible. This applies not only to information, but also to the machines on the network and other aspects of the technology infrastructure. This inability to access the required resources is called "denial of service".

Virus and worms:

A virus is a collection of programs, which are designed to replicate, attach to other programs, and perform unsolicited and malicious actions. The different types of virus are

- **Boot Sector virus:** Boot Sector virus infects the master boot record of a computer system. This virus either moves the boot record to another sector on the disk or replaces it with the infected one.
- **File- Infecting virus:** File Infecting virus infects files with extension. Com and exe. This type of virus usually resides inside the memory and infects most of the executable files on a system. The virus replicates by attaching a copy of itself to an uninfected executable program.
- **Polymorphic virus:** Polymorphic virus unlike other viruses consists of static virus program that gets copied from file as it propagates. Such virus is difficult to detect because each copy it generates appears different from the other one.
- **Stealth virus**: Stealth virus read system files or system sectors and when some other program requests for information from portions of the disk, it changes back into the correct form. Use of stealth virus is the major reason why most antivirus programs operate best when the system is started from a known-clean floppy disk. When this happens, the virus does not gain control over the system and is immediately available to be seen and dealt with. The stoned monkey virus is an example of stealth virus.
- **Multipartite virus:** - Multipartite virus infects both boot sectors and executable files and uses both machines to spread. It is the worst virus of all because it can combine some or all of the stealth techniques along with polymorphisms to prevent detection. For example, if a user runs and application infected with a multipartite virus, the virus activates and infects the hard disk's master boots records. Moreover, the next time the computer starts, the virus gets activated again and starts infecting virus gets activated again and starts infecting every program that the user runs.

Worms: -

Worms are the programs constructed to infiltrate and on the legitimate date processing programs and alter or destroy data. They often use network connection to spread from one computer system to another, thus, worms attack system that are linked through communication lines.

The reduce themselves, worms make use network medium such as -

- Network mail facility, in which a worm can mail a copy of itself to other system.
- Remote execution capability, in which a worm can execute a copy of itself on another system
- Remote log of capability, where by a worm can log into a remote system as a user and then use commands to copy itself from one system to another.

The worm's replication mechanism can access the system by using any of the three methods given below-

- It employs password cracking, in while it attempts to log into systems using different passwords such as words from an online dictionary.
- It exploits a trap door mechanism in mail programs, which permits it to send commands to a remote systems command interpreter.
- It exploits a bag in a network, information program, which permits it to access a remote system's command interpreter.

Tarzan horse:

A Tarzan Horse is a destructive program, which is concealed in a piece of software. It enters into a computer through an e- mail or free programs that have been downloaded from the Internet. Once it get into the computer, it usually opens the way for other malicious software (like viruses) to enter into the computer system. It may also allow unauthorized users to access the information stored in the computer.

Logic bomb:

A logic bombs is program or portion of a program, which lies dormant until a specific part of program logic is activated. The most common activator for logic bomb is a date. The logic bomb checks the computer system date and does nothings until a pre-programmed date time is reached.

Antivirus: -

Antivirus software has normally a built-in scanner, which scans all files on the computers hard disk's it looks for changes an activities in computers typical in case of a virus attack. They look for particular types of code within programs. The software generally relies on having prior knowledge of the virus. As a result, frequent update to the tools is necessary. The important thing to be aware of the possibility of an attack to possess a good virus checking software and to have data backup.

Digital Signature:

Digital signature is used to verify the authenticity of electronic document. In other words, digital signatures play the role of physical signature is verifying electronic documents. It uses PKC technique, which employs an algorithm using two different but mathematically related keys, one for creating a digital signature or transferring data into seemingly unintelligible form and another key for verifying a digital signature or returning the message to its original form.

To understand the concept of digital signature in a better way, we must first know the legal implications of digital signature. A signature is not part of substance of a transaction but is a representation. Signature serves the following general purposes.

Evidence: - A Signature authenticates writing by identifying the singer with the signed document.

Ceremony: - The act of singing a document cells to the signer's attention towards the legal significance of the signer's act, and thereby helps preventing inconsiderate engagements.

Approval: - In certain contents defined by low or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it has legal effect.

Efficiency and Logistics: - A signature on a written document often imparts a sense of clarity and finality to the transaction and may lesson the subsequent need to inquire beyond the face of a document.

To achieve the basic purpose of signatures outlined above, a signature must have the following attributes: -

Signer Authentication: - A signature should indicate who signed a document, message or record and should be difficult for another person to produce without authorization.
Document Authentication: - A signature should identify what is signed, making it impracticable to falsify or alter either the signed matter of the signature without detection.

Firewall: -

The ongoing occurrences of incidents patterning to network security caused a great concern to the people, using computers as their medium to exchange data across the country. A need was felt for a method of controlling the traffic, which allows access of information to computer. Organizations required on application that could protect and isolate their internal systems from the Internet. This application is called Firewall.

Generally, Firewall system comprises software computer, host, or a collection of lots set up specifically to shield a site or subnet from protocols and services that can be a threat from hosts outside the subnet. It serves as the gatekeeper between an entrusted network (Internet) and the more trusted internal networks.

Firewall provides the protection against the following: -

- Block unwanted traffic.
- Direct incoming traffic to more trustworthy internal system.
- Hid vulnerable system, which can not be secured from the Internet.
- Log traffic to and from the private network.
- Hide information like system names, network Topology, network, network device types and Internet user ID' from the Internet.

Types of Firewall: -

A Firewall intercepts the data between the Internet and the computer. All data traffic passes through it, and it allows only authorized data to pass into the corporate network. Firewall is typically implemented using one of the three primary architectures: -

1. Packet Filtering.
2. Application- level gets way.
3. Circuit level gets way.

Hacker and Cracker: -

The term hacker refers to the person with the intention of finding some weak points in the security of websites and other computer system in order to gain unauthorized access. The activities of hackers are not limited to only gaining the unauthorized access to system, but also include stealing and