**INFORMATION TECHNOLOGY ACT (SELF STUDY COURSE)**

**1)Write about Cyber Law and its objectives. Also give an overview on Information Technology Act.**

Cyberlaw:

The field of law dealingwith the Internet,encompassing cases,statutes, regulations,and disputes that affectpeople and businessesinteracting throughcomputers. Cyberlawaddresses issues of onlinespeech and business thatarise because of the natureof the medium, includingintellectual property rights,free speech, privacy,

e-commerce, and safety, aswell as questions ofjurisdiction.

In addition to regulating the overall internet’s happenings and crimes, cyber law recognizes popular usages, which include e-documents. Earlier, contracts, agreements, or anything of a legal nature was made on paper. With the recognition of e-documents and digital signatures, the world is moving fast toward a paperless future. Since this reduces the use of paper and increases sustainability, these processes are widely encouraged by several environmental enthusiasts.

OBJECTIVES OF CYBER LAW:

Lawmakers have executed cyber law legal protections with the following objectives: The following features of cyber law make the internet a much safer place to explore:

* To be a safety net against online data predators.
* To ensure justice for cybercrime victims
* To prevent debit card or credit card fraud. Many people have switched to digital payment methods. Cyberlaw tries to make sure that victims do not have to go through the additional agony of long procedures.
* To block transactions when there is any unusual activity such as the input of an incorrect password.
* To ensure the safety of protected data. By knowing what cyber law is, one can easily adopt preventative measures.
* To ensure national security.

INFORMATION TECHNOLOGY ACT:

❖ Introduction: The Information Technology Act, 2000 provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce”, which involve the use of alternatives to paperbased methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend The Indian Penal Code, The Indian Evidence Act, 1872, The Banker’s Books Evidence Act, 1891 and The Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. The Information Technology Act, 2000 extend to the whole of India and it applies also to any offence or contravention there under committed outside India by any person.

❖ Salient Features of The Information Technology Act, 2000:

The salient features of The IT Act, 2000 are as follows –

▪ Digital signature has been replaced with electronic signature to make it a more technology neutral act. ▪ It elaborates on offenses, penalties, and breaches

▪ It outlines the Justice Dispensation Systems for cyber-crimes.

▪ The Information Technology Act defines in a new section that cyber café is any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.

▪ It provides for the constitution of the Cyber Regulations Advisory Committee.

▪ The Information Technology Act is based on The Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Bankers’ Books Evidence Act, 1891, The Reserve Bank of India Act, 1934, etc.

▪ It adds a provision to Section 81, which states that the provisions of the Act shall have overriding effect. The provision states that nothing contained in the Act shall restrict any person from exercising any right conferred under the Copyright Act, 1957.

**2)Explain the types of Intellectual Property Rights**.

**1. The Copyrights Act, 1957 (“Copyright Act”)**

Copyright protects the expression of an idea rather than the idea itself. Under section 13 of the Copyright Act, a protection under copyright can be obtained for ‘original literary, dramatic, musical and artistic works; cinematograph films; and sound recording’. Interestingly, a copyright protection can also be obtained for computer programmes. A copyright is an ‘exclusive right’ that is granted to a person to do or authorize to carry out certain activities with regards the copyrighted work.

The Copyright Act, under section 17, clearly states that the author of the original work (for which protection under copyright has been obtained) shall be the first owner of the work. Further, the owner has the right to license the copyright of their work to third-parties through a written agreement.

**2. The Trade Marks Act, 1999 (“Trade marks Act”)**

The Trade Marks Act, under section 2(zb) defines a ‘trade mark’ as ‘a mark capable of being represented graphically and which is capable of distinguishing the goods or services of one person from those of others and may include shape of goods, their packaging and combination of colours…’. In simpler words, a trademark provides protection for symbols, colours, shapes, words, etc. representing and relating to a good or a service.

Interestingly, a trademark application need not be filed in respect of marks which are in use (but can also be filed in respect of marks which are intended to be used in the future). The primary requirements for registration of a trademark includes that it should consist of a mark capable of distinguishing the goods/services from those of others and that it is capable of graphical representation. The Trade Marks Act provides for absolute grounds of refusal of registration such as – (a) the mark not having a distinctive character; (b) a mark being deceptive and confusing to the public; (c) if a mark is hurtful to religious sentiments; (d) the mark is offensive, scandalous, or obscure, etc. In addition to the absolute grounds of refusal, the statute also provides for relative grounds of refusal of registration (viz. similarity with pre-existing marks).

**3. The Patents Act, 1970 (“Patents Act”)**

A ‘Patent’ is an intellectual property right which protects any new invention. It is an exclusive right that protects the rights of the inventor and prevents other people to unauthorizedly use and misappropriate the registered patent.

A patent is granted for a term of 20 (twenty) years from the date of filling of the application. It is important to note that patent for a new invention is registered only if the invention is ‘novel’ and ‘original’ i.e. it has not been introduced in the public domain in India or anywhere in the world; is ‘capable of industrial application’ which refers to the ability of the invention to be used in an industry; and is an invention that requires to employ a process of ‘inventive steps’, which is defined as ‘a feature of an invention that involves technical advance as compared to the existing knowledge or having economic significance or both and that makes the invention not obvious to a person skilled in the art’, under the Patents Act.

The Patents Act bestows each inventor, whose patent has been registered, with certain rights, namely:

* with respect to a patent for a product, the right to prevent third parties form using, selling, making, importing, etc. the product without prior consent; and
* with respect to a process for which a patent is obtained, the right to prevent third parties from using, selling, offering, etc. a product obtained from that process, without the prior consent of the original inventor.

**4. The Design Act, 2000 (“Design Act”)**

A ‘design’ under the Designs Act [section 2(d)] means and includes ‘only the features of shape, configuration, pattern, ornaments or composition of lines or colours, applied to any article whether in two dimensional or three dimensional or in both forms, by any industrial process or means, whether manual, mechanical or chemical, separate or combined, which in the finished article appeal to an are judged solely by the eye’.

An application for registration of an industrial design is to be made to the Controller- General of Patents, Designs and Trade Marks. However, a design shall only be considered for registration if – (a) it is novel and an original innovation i.e., it has not been produced before or reproduced by anyone; (b) it has not been disclosed to the public anywhere in India or outside the jurisdiction of India; and (c) it can be easily distinguished from other known designs.

Furthermore, once a design is registered, the registered proprietor is afforded protection for an initial period of 10 (ten) years, which is extendable (upon filing an application for extension) for a further period of 5 (five) years.

**5. The Geographical Indications of Goods (Registration and Protection) Act, 1999 (“GI Act”)**

Many goods in India are widely popular owing to their place of origin. For instance, ‘Darjeeling tea’ is unique and popular owing to many factors including but not limited to its origin, the skill set of the tea farmers of Darjeeling and the weather prevailing in that area. Other such examples of products which have a bearing of the place of origin (or factors specific to the place of origin includes Banarsi Saree; Basmati Rice, etc).

A ‘Geographical Indication’ is defined as ‘an indication which identifies such goods as agricultural goods, natural goods or manufactured goods as originating, or manufactured in the territory of country, or a region or locality in that territory, where a given quality, reputation or other characteristic of such goods is essentially attributable to its geographical origin and in case where such goods are manufactured goods one of the activities of either the production or of processing or preparation of the goods concerned takes place in such territory, region or locality as the case may be’. The GI Act covers only goods such as agricultural goods, food stuff, handicraft goods, manufactured goods, and natural goods.

An application for registering a good under the GI Act requires a statement explaining how the geographical indication affects to the origin of the good in terms of the quality, characteristics, and reputation of the good; the class of goods; particulars with regards the appearance of the geographical indication and the map of the territory/area/country where the good has originated.

**6. The Protection of Plant Varieties and Farmer’s Rights Act, 2001 (“Plant Varieties Act”)**

The objective of the Protection of Plant Varieties and Farmer’s Right Act, 2007, is to recognize rights of Indian farmers and to provide protection to plant varieties in order to encourage the growth and development of more plant varieties.

In 1994, India became a member to the Trade Related Aspect of Intellectual Property Rights Agreement (TRIPS) under which all members are required to accommodate and provide for the protection of plant varieties [Article 27(3)(b) of TRIPS]. All plant varieties that have been registered and awarded protection are entered and recorded into the National Register of Plant Varieties.

The Plant Varieties Act permits any breeder, farmer and any person as authorized, to apply for registration of a new plant variety. A new plant variety is registrable if it satisfies the conditions of ‘novelty, distinctiveness, uniformity and stability’. To elaborate, the condition of novelty requires that at the date of filing the application (for protection), the plant variety must not be sold. Further, distinctiveness encompasses the requirement of having at least one distinguishing factor from all other existing and protected plant varieties. The requirement of uniformity means that all essential characteristics of the plant variety must be uniform. Lastly, the plant variety being registered for is required to be ‘stable’, meaning that the essential characteristics of the plant variety must remain unchanged after repeated propagation of such plant variety.

**7. The Semiconductor Integrated Circuits Layout- Design Act, 2000 (“SICLD Act”)**

A ‘semiconductor integrated circuit’ is defined as ‘a product having transistors and other circuitry elements which are inseparably formed on a semiconductor material or an insulating material or inside the semiconductor material and designed to perform an electronic circuitry function’.

Under the SICLD Act, all layout-designs capable of being registered are required to be original; commercially unexploited anywhere in India and in any convention countries; inherently distinctive and inherently distinguishable from other registered layout- designs. An application for registration of design layouts has to be in writing and is required to be filed before the Registrar in the Semiconductor Integrated Circuits Layout-Design Registry present in the territorial limits of the principal place of business of the applicant.

Further, the protection afforded to registered layout-designs is for a period of 10 (ten) years.

**3)Elaborate Strategy-3, 4 and 5 for Cyber Security**

Strategy 3 − Encouraging Open Standards

Standards play a significant role in defining how we approach information security related issues across geographical regions and societies. Open standards are encouraged to −

* Enhance the efficiency of key processes,
* Enable systems incorporations,
* Provide a medium for users to measure new products or services,
* Organize the approach to arrange new technologies or business models,
* Interpret complex environments, and
* Endorse economic growth.

Standards such as ISO 27001[3] encourage the implementation of a standard organization structure, where customers can understand processes, and reduce the costs of auditing.

Strategy 4 − Strengthening the Regulatory Framework

The objective of this strategy is to create a secure cyberspace ecosystem and strengthen the regulatory framework. A 24X7 mechanism has been envisioned to deal with cyber threats through National Critical Information Infrastructure Protection Centre (NCIIPC). The Computer Emergency Response Team (CERT-In) has been designated to act as a nodal agency for crisis management.

Some highlights of this strategy are as follows −

* Promotion of research and development in cybersecurity.
* Developing human resource through education and training programs.
* Encouraging all organizations, whether public or private, to designate a person to serve as Chief Information Security Officer (CISO) who will be responsible for cybersecurity initiatives.
* Indian Armed Forces are in the process of establishing a cyber-command as a part of strengthening the cybersecurity of defense network and installations.
* Effective implementation of public-private partnership is in pipeline that will go a long way in creating solutions to the ever-changing threat landscape.

Strategy 5 − Creating Mechanisms for IT Security

Some basic mechanisms that are in place for ensuring IT security are − link-oriented security measures, end-to-end security measures, association-oriented measures, and data encryption. These methods differ in their internal application features and also in the attributes of the security they provide. Let us discuss them in brief.

Link-Oriented Measures

It delivers security while transferring data between two nodes, irrespective of the eventual source and destination of the data.

End-to-End MeasuresIt is a medium for transporting Protocol Data Units (PDUs) in a protected manner from source to destination in such a way that disruption of any of their communication links does not violate security.

Association-Oriented Measures

Association-oriented measures are a modified set of end-to-end measures that protect every association individually.

Data Encryption

It defines some general features of conventional ciphers and the recently developed class of public-key ciphers. It encodes information in a way that only the authorized personnel can decrypt them.

**4)What is Network Security? Describe Types of Network security devices.**

The word "network security" refers to the tools, techniques, and policies used to monitor, detect, and respond to illegal network intrusions and safeguard digital assets, such as network traffic. When it comes to protecting your network, hardware and software solutions (and resources like knowledgeable security analysts, hunters, and incident responders) are all part of the solution.

To protect the network against cyber attacks, hackers, and staff irresponsibility, network security is employed. Hardware, software, and cloud services all play a role in ensuring the safety of your network.

TYPES OF NETWORK SECURITY DEVICES:

### 1. Firewall[​](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#1-firewall)

Incoming and outgoing traffic on a network is controlled by firewalls, which have established security policies. [Firewalls](https://www.zenarmor.com/docs/network-security-tutorials/what-is-firewall) protect your computer from unwanted traffic and are an essential component of any modern computing environment. Firewalls, particularly Next-Generation Firewalls([NGFWs](https://www.zenarmor.com/docs/network-security-tutorials/next-generation-firewall)), play a critical role in network security, preventing malware and application-layer attacks.

#### **A. Packet-filtering firewall**[**​**](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#a-packet-filtering-firewall)

The first and simplest [type of firewall](https://www.zenarmor.com/docs/network-security-tutorials/what-are-the-types-of-firewalls) is one that filters packets. At the network layer, they merely compare the source and destination IP addresses, protocol, and source/destination port of a data packet against set rules to determine whether or not to allow or refuse it. [Packet filtering firewalls](https://www.zenarmor.com/docs/network-security-tutorials/what-is-packet-filtering-firewall) are inherently stateless, which means they monitor each packet independently without keeping track of the established connection or packets that have gone through it previously. As a result, the capacity of these firewalls to defend against sophisticated threats and assaults is significantly compromised.

#### **B. Proxy firewall**[**​**](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#b-proxy-firewall)

Proxy firewalls, also known as application-level gateways, are constructed via an application-layer proxy server. Instead of directly connecting to the internal network, the connection is established through the proxy firewall. The [proxy firewall](https://www.zenarmor.com/docs/network-security-tutorials/what-is-proxy-firewall) will initially receive a request from an external client. The proxy firewall then checks the request's legitimacy before sending it on behalf of the client to one of the internal devices. An internal client may also request website access, with the proxy device sending the request while concealing the client's name and location. Consequently, one of the primary benefits of proxy firewalls is the provision of privacy.

#### **C. Stateful packet-filtering firewall**[**​**](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#c-stateful-packet-filtering-firewall)

Stateful inspection firewalls inspect packets in addition to validating and recording existing connections to provide more robust and comprehensive protection. After establishing a connection, they generate a state table including the source/destination IP addresses and source/destination ports. Rather than relying on a hard-coded set of rules based on this information, they generate their own rules dynamically to enable the prediction of incoming network traffic. Not-belonging-to-a-verified-active-connection data packets are conveniently refused. Stateful firewalls feature significant logging capabilities that may be employed for monitoring and troubleshooting.

#### **D. Web application firewall (WAF)**[**​**](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#d-web-application-firewall-waf)

A web application firewall or [WAF](https://www.zenarmor.com/docs/network-security-tutorials/what-is-waf) aids in the protection of web applications by filtering and monitoring HTTP traffic between a web application and the Internet. It generally protects online applications from several threats, including cross-site forgery, cross-site scripting ([XSS](https://www.zenarmor.com/docs/network-security-tutorials/what-is-cross-site-scripting-xss)), file inclusion, and SQL injection. A WAF is protection at protocol layer 7 (in the OSI model) and is not meant to guard against all forms of assaults. Typically, this technique of attack mitigation is part of a suite of technologies that, when combined, provide comprehensive protection against a variety of attack vectors.

By placing a WAF in front of a web application, the application is protected from the Internet. A proxy server protects the identity of a client machine by acting as an intermediary, whereas a WAF is a form of reverse proxy that shields the server from exposure by requiring clients to pass through it before contacting the server.

### 2. Antivirus[​](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#2-antivirus)

Malware and other potentially harmful applications may be detected and removed using an antivirus tool. It was formerly possible to employ [antivirus](https://www.zenarmor.com/docs/network-security-tutorials/what-is-antivirus) software to protect against only viruses. As a result, they now protect from malware, ransomware, and spyware, among other threats. In some cases, email phishing attempts can also be prevented by antivirus software. Network security devices and tools should be able to detect threats from any source, including dangerous programs and viruses via email.

### 3. Intrusion detection system (IDS)[​](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#3-intrusion-detection-system-ids)

IDS is a hardware or software program that monitors a network for harmful activities or policy breaches, such as phishing. A security information and event management system is often used to report or gather any harmful activity or violation. Some intrusion detection systems ([IDS](https://www.zenarmor.com/docs/network-security-tutorials/what-is-intrusion-detection-system)) can respond immediately to intrusion detection.

Two major kinds of intrusion detection software systems exist host-based and network-based. These categories correspond to the placement of IDS sensors (on a host/endpoint or a network).

Some specialists categorize the market even further, citing perimeter IDS, VM-based IDS, stack-based IDS, signature-based IDS, and anomaly-based IDS (with acronyms matching the IDS' descriptive prefixes).

#### **A. Intrusion Protection Systems (IPS)**[**​**](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#a-intrusion-protection-systems-ips)

When harmful behavior is detected on a network, an intrusion prevention system ([IPS](https://www.zenarmor.com/docs/network-security-tutorials/what-is-ips)) takes action to prevent it, such as reporting, blocking, or dropping it. IPSs can be hardware or software.

Intrusion detection systems (IDS) can only identify harmful behavior, but they can't do anything about it other than inform an administrator. Next-generation firewalls and unified threat management (UTM) solutions often include intrusion prevention systems as an optional component. They must be strong enough to scan a large volume of traffic without slowing down network performance, like many other network security systems.

#### **B. Host-based intrusion detection systems**[**​**](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#b-host-based-intrusion-detection-systems)

HIDS is an acronym for "host-based intrusion detection system," a program that keeps an eye on a computer or network for any unusual behavior, such as invasions from outside or internal misuse of resources or data.

HIDS software, like a home security system, tracks abnormal activities and alerts network administrators. When using HIDS tools, you may easily search through the log files created by your apps to look for indicators of an intrusion and other irregularities. Automated detection is the primary purpose of HIDS tools, which eliminates the need to manually search through log files once they've been sorted and processed.

#### **C. Network-based intrusion detection systems**[**​**](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#c-network-based-intrusion-detection-systems)

A NIDS is a type of network intrusion detection system (NIDS) in which devices are intelligently dispersed throughout a network and passively monitor the traffic passing over them. NIDS can be hardware or software-based systems and can connect to various network media, such as Ethernet, FDDI, and others, depending on the manufacturer of the system. NIDS typically feature two network ports. Promiscuous mode listening and control and reporting are the primary functions of these tools.

### 4. Unified Threat Management (UTM)[​](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#4-unified-threat-management-utm)

UTM is an information security word that refers to a single security solution, and typically a single security appliance, that delivers numerous network security functions at a single location. Antivirus, anti-spyware, anti-spam, network firewalling, intrusion detection and prevention, content filtering, and leak protection are typical features of a UTM device. Some devices additionally include remote routing, network address translation ([NAT](https://www.zenarmor.com/docs/network-basics/what-is-nat)), and support for virtual private networks (VPN). The solution's appeal is built on its simplicity, so enterprises that previously had different suppliers or appliances for each security activity can now have them all under a single vendor, backed by a single IT team or division, and managed from a single interface.

### 5. Wireless Intrusion Prevention and Detection System (WIDPS)[​](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#5-wireless-intrusion-prevention-and-detection-system-widps)

As specialized security equipment or integrated software program, the wireless intrusion prevention system (WIPS) is responsible for keeping an eye on the radio spectrum in the vicinity of the wireless network for any rogue access points or other dangers.

An administrator is alerted when a difference is identified between the MAC addresses of all wireless access points on a network and the known signatures of pre-authorized, known wireless access points. WIPS capable of analyzing the unique radio frequency signatures generated by wireless devices can avoid MAC address spoofing by blocking unfamiliar radio fingerprints.

### 6. Network Access Control (NAC)[​](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#6-network-access-control-nac)

These NAC systems provide visibility and access management for business networks by enforcing policies on devices and users.

Because of the increasing number of mobile devices connecting to networks and posing security concerns, businesses must have the tools necessary to monitor, manage access to, and ensure compliance with their network security policies. Using a [NAC](https://www.zenarmor.com/docs/network-security-tutorials/what-is-network-access-control-nac) system, insecure nodes can't get access to the network by being blocked from using it, isolated, or given only limited access to computing resources.

### 7. Network Load Balancer (NLB)[​](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#7-network-load-balancer-nlb)

A Network Load Balancer operates at the Open Systems Interconnection (OSI) model's fourth layer. It is capable of processing millions of queries per second. After receiving a connection request, the [load balancer](https://www.zenarmor.com/docs/network-security-tutorials/what-is-load-balancing) picks a target from the target group for the default rule. It tries to establish a TCP connection with the given destination on the port specified in the listener settings.

NLB is created particularly for high-performance online traffic that is not typical. NLB can handle millions of queries per second while retaining extremely low latency.

### 8. Web Filter[​](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#8-web-filter)

The primary purpose of a [web filtering](https://www.zenarmor.com/docs/network-security-tutorials/what-is-web-filtering) device is to improve online security, but it also provides some useful secondary benefits. A web content filter equipment stops Internet users from accessing websites that host malware and ransomware. It protects organizations, networks, and users from a variety of web-based threats and decreases the chance of a financial or data loss resulting from acts of cybercriminals.

In the workplace, web content filtering appliances can be configured to prevent employees from visiting non-work-related websites and "cyberslacking", thereby increasing productivity. In any public Internet access location (such as a store, a school, or a workplace), a web content filter appliance can prevent customers, students, diners, and employees from being exposed to inappropriate online content.

### 9. Spam Filter[​](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#9-spam-filter)

[Spam filtering](https://www.zenarmor.com/docs/network-security-tutorials/what-is-spam-filtering) solutions were created to assist consumers to detect, identifying, and avoiding unsolicited emails. Today, the majority of anti-spam companies utilize effective email filters to classify messages, hence enhancing email deliverability. Here is a list of the most prevalent anti-spam filters:

* These filters prevent [spam](https://www.zenarmor.com/docs/network-security-tutorials/what-is-spam-email) from accessing your email by employing user-defined criteria.
* Bayesian filters - one of the most powerful filters ever created - employ cutting-edge technology to examine the statistical likelihood of every incoming communication.
* These filters examine the language and substance of communication to evaluate whether or not it is safe or spam.
* These filters block all emails from an individualized list of spammers known as a blacklist.
* Challenge-response filters - the primary function of a challenge-response filter is to verify that a human is transmitting the message.
* Before acquiring authorization to send an email, a challenge-response filter requires the sender to provide a code.

### 10. Proxy Server[​](https://www.zenarmor.com/docs/network-security-tutorials/network-security-devices#10-proxy-server)

A [proxy server](https://www.zenarmor.com/docs/network-security-tutorials/what-is-proxy-server) is a system or router that gives access to the Internet to users. Consequently, it prevents cybercriminals from infiltrating a private network. It is a server that acts as a middleman between end-users and the websites they visit online.

When a computer connects to the internet, an IP address is utilized. This is analogous to your residence's street address, directing incoming data to its destination and identifying outgoing data with a return address for other devices to validate. A proxy server is simply a computer with its IP address on the Internet.

There is more than one kind of forward HTTP proxy to select from, based on your requirements. The level of privacy they give is the key distinction between these proxy server categories:

* Transparent proxy: A transparent proxy does not provide any enhanced privacy or security. Web servers receive your true IP address and are aware of your proxy connection when you use a proxy.
* Anonymous proxies: Anonymous proxies guarantee that they will not transmit your IP address to the websites and services that you use. Websites will receive a spoofed IP address instead of your genuine one, which is why anonymous proxies are also known as distorting proxies.
* High anonymity proxies: Consider high anonymity proxies, also known as elite proxies, an upgrade from your typical anonymous proxy. The foundations are the same, but high anonymous proxies further conceal your usage of the proxy. If you use one of these, a website will be unable to identify your proxy usage.

**5)Write about Signatures in Cyber Law**

A signature is a depiction of the handwritten name or identity of an individual to show his unique identification on any document file etc. For an individual signature is of utter importance in giving his consent on any document. In recent times, traditional signatures have been replaced by electronic and digital signatures. It is pertinent to note that with new innovations and technology in different fields there is a tremendous increase in online transactions that causes transfer of online payment and document sharing in everyday life. Present-day sharing documents are done through email etc. There emerged a new mode to sign the document and this mode is called the e-signature or digital signature.

#### **1.Digital Signature**

A digital signature is defined in [Section 2(1)(p)](https://indiankanoon.org/doc/1752240/) of the Information Technology Act,2000. A digital signature is a mathematical algorithm that is regularly used to validate the originality and if the message is true and genuine. A digital signature is a computerized fingerprint that is distinct to a person or independent organization and it is used to protect the information in the digital message or document. In the case of emails, the email itself becomes part of the digital signature. In simple words, a digital signature is a present-day alternative to the traditional way of signing documents on paper with ink.

A digital signature is a kind of electronic signature that is used to verify the name of the sender of a message or the signer of a document. It makes sure that the document or message is genuine and the documents that are sent are untouched. Digital signature gives 2 algorithms.

1. Private key or user secret key
2. Verifying signature that includes the user’s public key. The output of the signature process is called the digital signature.

### ****Digital Signature Certificate****

A digital signature certificate (DSC) is equal to a physical or paper certificate. DSC is a procedure to show the authenticity of electronic documents. It is needed to be presented electronically to show the identity, access information, or sign document digitally. The Central Government has appointed the Controller of Certifying Authority that will grant a license to the Certifying Authorities to issue DSC to the user.

### ****Types of Digital Signature Certificate****

There are 3 types of digital signatures based on security level i.e. [class 1, class 2, and class 3 certificate.](https://www.elock.com/Digital-signature-laws-in-India.php)

**Class 1 certificate:** It is not legally recognized. It is based on confirmation of valid email and not direct verification.

**Class 2 certificate:** This is based on the identification of the person that is required to be verified against a reliable pre-verified database.

**Class 3 certificate:** is a person in the presence of the Registration Authority proves his identity.

Lastly, businesses in India are using digital signatures to sign documents like invoices, reports, contracts, agreements, HR letters, and other such documents.

**Features of Digital Signature**

1. **AUTHENTICATION**

It means that the [digital signature](https://lawlex.org/lex-pedia/lex-articles/digital-signature-vs-electronic-signature/24123)will help the receiver to recognize who has sent the message or authenticate the source of the message.

1. **INTEGRITY**

It may be so that while sending the message the document may get altered in this case the receiver will be able to know the originality of the message.

1. **NON – REPUDIATION**

The sender cannot refuse that he did not send any message.

### ****2.Electronic Signature****

The electronic signature or e- signature is equal to that of a handwritten Signature under the Information Technology Act, 2000. Though there are few exceptions to it. The act permits signing any document using e-signature. An e-signature must meet certain conditions and it needs to be studied before it is used by any individual.

According to the US Federal ESIGN Act, electronic signatures are defined as: “Electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.”

#### **Two types of E-signatures**

1. Electronic signature joined with an Aadhar identity number with electronic know -your- customer (e-KYC) method. It is also known as e-sign online electronic signature service.
2. Digital signature is set up by an “asymmetric crypto-system and hash function”. The signatory is given 1-2 years of digital ID which is stored on a USD token, along with personal PIN to accent the document.

**Validity of Electronic Signature**

* Any person when signing a particular document with Electronic signature  his  ID has to be linked .
* Electronic signature is based on an audit trail.
* The person should have control over the date created that is being made to sign with an electronic signature.