B.Com(P) Semester-III Commerce

Skill Enhancement Course (SEC)
Cyber Crimes and Laws

Study Material : Unit I-V

दिल्ली विश्वविद्यालय UNIVERSITY OF DELHI

निष्ठा धृतिः सत्यम्

SCHOOL OF OPEN LEARNING
University of Delhi

Department of Commerce

CONTENTS

UNIT I CYBER CRIME

UNIT II DEFINITIONS UNDER IT ACT, 2000

UNIT III CONTEMPORARY BUSINESS ISSUES IN CYBER SPACE

UNIT IV ELECTRONIC RECORDS

UNIT V REGULATORY FRAMEWORK

Editor
Dr. U.S.Pandey

Written by
Guneet Kaur

SCHOOL OF OPEN LEARNING
University of Delhi
5, Cavalry Lane, Delhi-110007

Unit I

CYBER CRIME

- Cyber Crimes Introduction
- Computer crime and cyber crimes;
- Distinction between cyber crime and conventional crimes;
- Kinds of cyber crimes- cyber stalking,
    - cyber terrorism,
    - forgery and fraud,
    - crimes related to IPRs,
    - computer vandalism;
- cyber forensic
- Summary
- Exercise

1.1 CYBER CRIME INTRODUCTION

Computer crime is a growing threat to society caused by the criminals and irresponsible actions of individuals who are taking advantage of the widespread use of computer networks in our society. It presents a major challenge to the ethical use of information technologies.

1.1.1 COMPUTER CRIME

Computer crime poses serious threats to the integrity, safety, and survival of most e-business systems, and thus makes the development of effective security methods a top priority.

According to Association of Information Technology Professionals (AITP), computer crime includes the following:

- The unauthorized use, access, modification, and destruction of hardware, software, data, or network resources.
- The unauthorized release of information
- The unauthorized copying of software
- Denying an end user access to his or her own hardware, software, data, or network resources
- Using or conspiring to use computer or network resources to illegally obtain information or tangible property.

1.1.2 CYBER CRIME

Cyber-crime encompasses any criminal act dealing with computers and networks (called hacking). Cyber-crime includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber-crimes when the illegal activities are committed through the use of a computer and the Internet. Cyber-crimes also includes offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).

Cyber-crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyberwarfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court.

1.2 COMPUTER CRIME AND CYBER CRIME

Computer crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are subject everywhere to criminal sanctions. The term computer misuse and abuse are also used frequently but they have significantly different implications. Annoying behavior must be distinguished from criminal behavior in Law. As per IT Act, 2000, no description has been categorically made for computer crime and cyber-crime. So till today, it is very difficult to differentiate between these two words. In relation to the issue of intent, the principle of claim of right also informs the determinations of criminal behavior. For example, an employee who has received a password from an employer, without direction as to whether a particular database can be accessed, is unlikely to be considered guilty of a crime if he or she accesses those databases. So a distinction must be made between what is unethical and what is illegal, the legal response to the problems must be proportional to the activity that is alleged. Common types of computer crimes are:

- Forgery;
- Fraud by system manipulation intentionally;
- Any modification to data or programs or databases; and
- Accessing computers without authorization;

But cyber-crimes are somehow different from computer crimes. Computer crime happens in physical space with or without the network. Cyber-crime takes place in a virtual space through digital environment. Recent example of cyber-crime was Bazzee.com case, which is a MMS scandal. Cyber-crimes may happen globally as there is no geographical limit for cyberspace.

1.3 DISTINCTION BETWEEN CYBER CRIME AND CONVENTIONAL CRIMES

Although we talk about cybercrime as a separate entity to traditional crime, it is carried out by the same types of criminals for the same type of reasons. These hackers are professional thieves, criminal gangs, disgruntled employees, professional competition, activists, disillusioned youth and state adversaries. They have the same motivations as traditional criminals such as boredom and vandalism, ideological or political support, malice or revenge, monetary gain through extortion or sale of illegally obtained data, terrorism or notoriety and sensationalism. However, there are certain differences between cyber-crimes and conventional crimes, which are discussed below:

- **Evidence of the offences** - Traditional criminals usually leave traces of a crime, through either fingerprints or other physical evidences. On the other hand, cybercriminals rely on the Internet via which they commit their crimes, and it leaves very little evidence about the cybercrime. Forensic investigators usually experience great difficulty in gathering evidence that could lead to the conviction of cybercriminals since these criminals can freely change their identities. The Internet also allows the anonymity of its users, and this implies that cybercriminals can use any pseudonyms for their identification. On the other hand, it is difficult for traditional criminals to fake their gender, race, or age.
- **Length of investigations** - Since cybercrime involves perpetrators using falsified names and working from remote locations, it usually takes longer to identify the real cybercriminals and apprehend them. In most cases, cybercriminals (such as hackers) escape from arrest because the investigators cannot locate them. Traditional crimes take shorter time period to investigate because the criminals usually leave evidence that can be used to spot them. For instance, traditional criminals can leave evidence such as DNA, fingerprints, photographs and videos captured on surveillance cameras, or personal belongings such as identity cards, and this makes it easy for investigators to identify and capture the culprits. In addition, such evidence makes it easy for the judiciary to convict the offenders.
- **Constitutional law provisions** – Article 20(3) of the Indian constitution deals with privilege against self-incrimination. According to this article, "No person accused of any offence shall be compelled to be a witness against himself". Consequently, cybercriminals can use this legal provision to deny the investigators any incriminating evidence that could lead to the prosecution of the cybercriminals.

This implies that even in situations where cybercriminals are apprehended, the trial process may take long unless the investigators gathered irrefutable evidence about the crimes.

- **Use of force** - Most of the traditional crimes (such as rape, murder, arson, and burglary among others) involve the use of excessive force that results in physical injury and trauma on the victims. On the other hand, cybercrimes do not require the use of any force since the criminals merely use the identities of their victims to steal from them. For example, cybercriminals use spoofing and phishing to obtain personal information such as credit card numbers from their victims, or use encrypted emails to coordinate violence remotely.
- **Scale of attacks** – Cyber-attacks can be conducted on a scale not possible in the physical world. A traditional bank robber may only be able to hit one or two banks a week, a cyber-attack can target 100's if not 1000's of sites at once.
- **Reach of attacks** – Cyber-attacks can be performed from anywhere in the world; they can be performed anonymously and within jurisdictions where the consequences of those actions may not, or cannot, be addressed by the criminal justice system. Attackers are also able to extract far more data digitally than would ever be possible in the physical world. For example 1 gigabyte of data is approximately 4,500 paperback books. Think of how many gigabytes of data is held on a system, hackers can extract this within a matter of minutes.
- **Speed of attacks** – Cyber-attacks are conducted at machine speed; a criminal can write a piece of code that can target multiple sites in minutes.
- **Perception and media effect** – The public and media perception of cyber-crime is different from a conventional crime. When large financial institutions have been hacked the media has often wholly apportioned blame to the organizations' rather than the criminals, this would not be the case in a physical bank robbery.

1.4 KINDS OF CYBER CRIMES – CYBER STALKING

There are many types of cyber-crimes and the most common ones are explained below:

1.4.1 Cyber Defamation

Every individual has a private right to protect his reputation. Every individual has a right to its own personal space and he would not want others to interfere in that 'space'. However, a public right to freedom of speech and expression guaranteed under Article 19(1)(a) of the Constitution of India makes enforcement of our private right a challenge. A delicate balance has to be maintained. The law of defamation has been designed to protect the reputation of an injured person and provide such balance between private and public rights by giving him the right to sue for damages.

Defamation comprises of both slander (defamation by speaking) and libel (defamation by means of writing).Slander involves the oral "publication" of a defamatory remark that is heard by another, which injures the subject's reputation or character. Slander can occur through the use of a hand gesture or verbal communication that is not recorded. Libel, on the other hand, is the written "publication" of a defamatory remark that has the tendency to injure another's reputation or character. Libel also includes a publication on radio, audio or video. Even though this would be considered oral, or verbal, communication to someone it is actually considered to be libel because it is published in a transfixed form.

In the good old days, slander was more popular and possible. After the popularity of the printing press, one witnessed the increase in libel. With the advent of information technology and the Internet, libel has become much more common and of course, easier. In this context, arises cyber defamation. In simple words, it implies defamation by anything which can be read, seen or heard with the help of computers/technology. Since the Internet has been described as having some or all of the characteristics of a newspaper, a television station, a magazine, a telephone system, an electronic library and a publishing house, there are certain noticeable differences between online and offline attempt of defamation which makes the online defamation more vigorous and effective.

Quantitatively, a comment defaming a person can be sent to a large number of persons through e-mail by a click of the mouse. Much easier would be to publish it on a discussion board known to be visited by thousands of persons every day. On the number game, it is still more convenient to make available the defamatory sentence to millions of people by merely publishing it on the website. The number of people a comment defaming a person might reach is gigantic and hence would affect the reputation of the defamed person much more than would an ordinary publication.

Qualitatively, the impact of an online comment defaming a person would again depend upon the fact as to where it has been published. Putting a defaming message in specific a newsgroups (for example, a lawyer’s group in case one wants to defame a lawyer) would necessarily have a more effective negative impact on the reputation of the person being defamed rather putting the same on a ladies’ kitty party group.

1.4.2 Corporate Cyber Smear

Harmful, defamatory, insulting or offending online message has been termed as Corporate cyber smear. It is a false and disparaging rumour about a company, its management or its stock. This is commonly done through the internet via websites, blogs, forums, emails and instant messaging, chat rooms and now in the social networking sphere. This kind of criminal activity has been a concern especially in stock market and financial sectors where knowledge and information are the key factors for businessmen. Persons indulging in corporate cyber smear include disgruntled employees or insiders, ex-employees, envious ex-colleagues, impostors, competitors, creditors, and even those seeking a forum when they are denied employment or former shareholders.

False and defamatory statements made against Amazon Natural Treasures, Inc. led to a stock price decline from an April 1997, 52-week high of $3.56 per share to approximately 12 cents per share. The low stock price led to a delisting from the QTCB to the pink sheets. It transpired that the statements were made by the owner of Demonte & Associates, a New York public relations firm, who claimed that a collection agency was suing Amazon for about $7,000.

1.4.3 Forgery

Forgery is defined as the criminal act that includes the purposeful defrauding, misleading, deception, and misrepresentation of a product, service, or item with the intent to deceive. The scope forgery is a vast one; forgery can include the production of falsified documents, counterfeited items - products intended to resemble other products, and the misrepresentation of fraudulent identification.

The criminal act of forgery can take place in a variety of settings; however - with regard to identity theft - the act of unlawfully recreating the likeness of the signature belonging to another individual or entity with the intent of providing deceitful authorization for economic gain is one of the foremost methodologies undertaken. Desktop publishing systems, colour laser and ink-jet printers, colour copiers, and image scanners enable crooks to make fakes, with relative ease, of cheques, currency, passports, visas, birth certificates, ID cards, etc.

Forgery could be of various types:

- Electronic forgery - The misuse of computer networks, the internet, and various avenues within the online community in order to defraud potential victims of identity theft is classified as electronic – or online forgery. Electronic Forgery is quite common within the digital age, which can include the illegal and unlawful reproduction of endorsements in the form of electronic signatures in order to illicitly assume the identity of the victim of identity theft.
- Financial forgery - Criminal fraudulent activity applicable to the events involving the exchange and circulation of currency may be classified as financial forgery. Identity theft resulting from this type of forgery can occur in a variety of fashions, including fraudulent purchases through the use of finances – and financial information – belonging to the victims of this crime.
- Commercial forgery - Forgery involving business activities, commercial endeavours, or professional operation of the provision of products or services is classified as commercial forgery; items unlawfully purchased with illegal and illicit finances may result from identity theft.
- Governmental and administrative forgery - Administrative forgery includes the vast expanses of laws, acts, ordinances, and legislation; identity theft in an

administrative realm may include the unlawful duplication of documentation or the illegal officiating of government-mandated forms and requirements.

In order to prevent these forgeries, electronic identity theft need to be stopped. Due to technological innovation, electronic identity theft is considered by many to be one of the most recently-developed crimes, credited – in part - to the ongoing advent of computer-based technology. This type of technology relies heavily on the Internet and online activity, and as a result, regulations and oversight of this type of activity has been expressed in the spectrum of preventative measures involving the cessation of electronic identity theft.

Companies providing methods of Identity theft prevention have employed protective measures ranging from securing online perimeters to communicative transmission inquiring about the validity of unsubstantiated activity.These types of companies have found their respective niche within the prevention of identity fraud upon providing protection in lieu of infringing on personal privacy.

1.4.4 Cyber Pornography

Pornography literally means, "Writings, pictures or films designed to be sexually exciting". Developing, distributing and propagating the same over the Internet is termed as cyber pornography. This would include pornographic Web sites, pornographic magazines produced using computers to publish and print the material and the Internet to download and transmit pornographic pictures, photos, writings, etc. In recent times, there have been innumerable instances of promotion of pornography through the use of computers. Information technology has made it much easier to create and distribute pornographic materials through the Internet; such materials can be transmitted all over the world in a matter of seconds. The geographical restrictions, which hitherto prevented, to a certain extent, foreign publications to enter into local territories, have disappeared.

Two primary reasons why cyber pornography has, in recent years, gathered much attention of both the offender and user, are:

- Easy accessibility;
- Anonymity.

Individuals can easily view thousands of pornographic images day and night within the privacy of the four walls of their homes. The Internet has decreased the hurdle of shame that comes with purchasing pornographic materials in a shop or the embarrassment of being caught with physical hard copies of pornomaterials. The consumer of such publications is more comfortable in opening a website and viewing/watching. With availability of broadband connections and high downloading speeds, the demand, though privately, seems to have risen.

On the other hand, anonymity has encouraged the offender to come out with more explicit and real material with higher degrees of inducement. Anybody can upload information onto a website from anywhere with the entire world as its market/consumer. It is extremely difficult to pinpoint persons responsible for such activities. It is also important to note that in countries where certain degree of pornographic material is permitted to be published and distributed, offenders quite often publish their information online from such countries though knowing well that the online market extends well beyond the geographical boundaries.

What has, however, been most disturbing is the increase in child pornography. Child pornography is different from other pornography, and consequently receives more stringent legal treatment. It is distinguished as an issue of child abuse — in its production and/or in the way it is used by podophiles to desensitize their victims. The growth of the Internet has provided child pornographers with a distribution vehicle which is perceived to be relatively anonymous.

1.4.5 Cyber Stalking

Cyberstalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. A cyber stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected. Cyberstalking messages differ from ordinary spam in that a cyber stalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages.

In a variation known as corporate cyberstalking, an organization stalks an individual. Corporate cyberstalking (which is not the same thing as corporate monitoring of e-mail) is usually initiated by a high-ranking company official with a grudge, but may be conducted by any number of employees within the organization. Less frequently, corporate cyberstalking involves an individual stalking a corporation.

WHOA (Working to Halt Online Abuse), an online organization dedicated to the cyberstalking problem, reported that in 2001, cyberstalking began with e-mail messages most often, followed by message boards and forums messages, and less frequently with chat. In some cases, cyberstalking develops from a real-world stalking incident and continues over the Internet. However, cyberstalking is also sometimes followed by stalking in the physical world, with all its attendant dangers.

The reasons why cyber stalking today is a preferred mode of harassment are:

(a) Ease of communication

(b) Access to personal information: With a bit hacking expertise, one might easily be able to access personal information of a person which would help in further harassment.

(c) Anonymity: The cyber stalker can easily use an identity mask thereby safeguarding his real identity.

(d) Geographical location: In online cyber stalking, the cyber stalker can be geographically located anywhere.

(e) Ease of indirect harassment: The cyber stalker does not directly harass his victim. Rather, he would post such comments on a common discussion board that would prompt the other users to send messages to the victim under a misconceived notion.

There are a number of simple ways to guard against cyberstalking. One of the most useful precautions is to stay anonymous yourself, rather than having an identifiable online presence. Use your primary e-mail account only for communicating with people you trust and set up an anonymous e-mail account, such as Gmail or Yahoo, to use for all your other communications. Set your e-mail program's filtering options to prevent delivery of unwanted messages. When choosing an online name, make it different from your name and gender-neutral. Don't put any identifying details in online profiles.

Should you become the victim of a cyber stalker, the most effective course of action is to report the offender to their Internet service provider (ISP). Should that option be impossible, or ineffective, the best thing to do is to change your own ISP and all your online names.

1.4.6 Online Gambling

Gambling is illegal in many countries. Computer is a medium for the purposes of online gambling. The act of gambling is categorized as an offence in some countries and has a legal sanctity in others. The main concern with online gambling is that most virtual casinos are based offshore making them difficult to regulate. This means that people offer gambling services on the Internet from countries where gambling is permitted where players, from such countries where gambling is illegal, play and bet. It is in this situation that the Internet helps the gamblers to evade the law. Anyone with access to a personal computer and an Internet connection can purchase lottery tickets or visit gambling sites anywhere in the world. The world of online gambling, due to its anonymity, unfortunately has many other hazards like danger of illegal use of credit card or illegal access to bank account.

1.4.7 Online Sale of Illegal Articles

There are certain articles like drugs, guns, pirated software or music that might not be permitted to be sold under the law of a particular country. However, those who would want to sell such articles find Internet a safe zone to open up online shops. There are specific concerns with regard to increase in online sale of drugs. A simple Internet search will turn up dozens of Web sites that let anyone order drug-of-choice for home-delivery.

The sale of illegal articles on the Internet is also one of those computer crimes where the computer is merely a tool to commit the crime. The traditional crime is already not permissible under various statutes. However, it is being committed by using computer and through the Internet where one gets a better and bigger market along with the benefit of anonymity.

1.4.8 Cyber Fraud

Cyber fraud (or Internet fraud) refers to any type of deliberate deception for unfair or unlawful gain that occurs online. It involves the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them; for example, by stealing personal information, which can even lead to identity theft. A very common form of Internet fraud is the distribution of rogue security software. Internet services can be used to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. Research suggests that online scams can happen through social engineering and social influence. It can occur in chat rooms, social media, email, message boards, or on websites.

The most common form of cyber fraud is online credit card theft. Credit card fraud involves misusing someone else's credit cards for one's own benefit. This risk of credit card fraud has increased manifold especially after the advent of e-commerce. People purchase products online through their credit cards. The Web sites offering products for purchase require the credit card details of the online buyer so that the price can be credited to the card. In the process, the details of the credit cards are stored on the server of the online retailer. If one is able to access the servers containing the credit cards details of the online consumer, it is easy to collect those details and then use for one's own benefit in online transactions.

Online auction and retail schemes are other kind of cyber fraud. These schemes typically purport to offer high-value items – ranging from Cartier watches to computers to collectibles such as Beanie Babies – that are likely to attract many consumers. These schemes induce their victims to send money for the promised items, but then deliver nothing or only an item far less valuable than what was promised (e.g., counterfeit or altered goods).

Business opportunity or work at home schemes are another type of fraud. Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn a substantial amount of money in "work-at-home" ventures. These schemes typically require the individuals to pay money upfront, but do not deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business.

1.4.9 Online Investment Fraud

There are frauds committed in the case of online investment schemes. One such scheme is issuance of false stocks. In this scheme, the person, either authorized or unauthorized, gains access to the computer systems of a company and is able to issue stocks to themselves or any other person. For instance, two employees of Cisco Systems, Inc. a US company, illegally issued almost $8 million in Cisco stock to themselves. The total value of the Cisco stock that they took (at the time that they transferred the stock) was approximately

$7,868,637. Both were sentenced to 34 months each in federal prison, restitution of $7,868,637 and a three year's period of supervised release.

Market manipulation scheme is another online investment fraud. Enforcement actions by the US Securities and Exchange Commission and criminal prosecutions indicate that the basic method for criminals to manipulate securities markets for their personal profit is the so-called "pump-and-dump" scheme. In this scheme, they typically disseminate false and fraudulent information in an effort to cause dramatic price increases in thinly traded stocks or stocks of shell companies (the 'pump'), then immediately sell off their holdings of those stocks (the 'dump') to realize substantial profits before the stock price falls back to its usual low level. Any other buyers of the stock who are unaware of the falsity of the information become victims of the scheme once the price falls.

Pyramid or Ponzi Scheme and chain letters is another online investment fraud. It is well suited to the Internet because they entice investors with the promise of quick profits using a home computer. Investors make money by recruiting new investors. The programme soon runs out of new investors and most of the players lose their money they invested. Chain letter schemes ask participants to send money to the name at the top of a list with the promise that they will eventually receive thousands of dollars when their name comes to the top.

Fraudulent financial solicitation is another online investment fraud. Due to its ease and anonymity, there have been instances of people soliciting money online for charitable purposes. One might seek financial contribution via credit card online to certain public purpose funds or schemes for the benefit of certain classes or down-trodden people of society. Many a time, fiscal statutes provide for income tax exemption for such contributions and online promises are made to provide a tax exemption certificate in case such contributions are made. The website may even provide for a printout of a fake certificate.

1.4.10 Spam and Phishing

Spamming and phishing are two very common forms of cybercrimes. There is not muchpeople can do to control them. Spam is basically unwanted emails and messages. They use Spambots. Phishing is a method where cyber criminals offer a bait so that people take it and give out the information that cyber criminals want. The bait can be in form of a business proposal, announcement of a lottery to which people never subscribed, and anything that promises them money for nothing or a small favor. There are online loans companies too, making claims that people can get insecure loans irrespective of their location. Doing business with such claims, people sure suffer both financially and mentally in the end.

Such spamming and phishing attempts are mostly emails sent by random people whom othersnever hear of. People should stay away from any such offers especially when they feel that the offer is too good. The US Cybercrime Center says – do not get into any kind of agreements that promise something too good to be true. In most cases, they are fake offers aiming to get people's information and to get their money directly or indirectly.

1.4.11 Spear Phishing

As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

Visiting West Point teacher and National Security Agency expert Aaron Ferguson calls it the "colonel effect." To illustrate his point, Ferguson sent out a message to 500 cadets asking them to click a link to verify grades. Ferguson's message appeared to come from a Colonel Robert Melville of West Point. Over 80% of recipients clicked the link in the message. In response, they received a notification that they'd been duped and warning that their behavior could have resulted in downloads of spyware, Trojan horse s and/or other malware.

Most people have learned to be suspicious of unexpected requests for confidential information and will not divulge personal data in response to e-mail messages or click on links in messages unless they are positive about the source. The success of spear phishing depends upon three things:

- The apparent source must appear to be a known and trusted individual
- There is information within the message that supports its validity, and
- The request the individual makes seems to have a logical basis.

Here's one version of a spear phishing attack: The perpetrator finds a web page for their target organization that supplies contact information for the company. Using available details to make the message seem authentic, the perpetrator drafts an e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator. The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming. If a single employee falls for the spear phisher's ploy, the attacker can masquerade as that individual and use social engineering techniques to gain further access to sensitive data.

1.4.12 Cyber Terrorism

According to the U.S. Federal Bureau of Investigation, cyberterrorism is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents". It is the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives. Cyberterrorism is sometimes referred to as electronic terrorism or information war.

Unlike a nuisance virus or computer attack that results in a denial of service, a cyberterrorist attack is designed to cause physical violence or extreme financial harm. According to the U.S. Commission of Critical Infrastructure Protection, possible cyberterrorist targets include the banking industry, military installations, power plants, air traffic control centers, and water systems.

Cyber terrorism can occur over the public internet, over private computer servers, or even through secured government networks. There are many ways in which a criminal could use electronic means to incite fear and violence. It is far less expensive to purchase a computer than to access guns or bombs, making this approach appealing for many potential criminals worldwide. It can be anonymous and conducted at a great distance away from the target. For just a few examples, consider these situations:

- Foreign governments may use hackers to spy on other countries intelligence communications in order to learn about where their troops are located or otherwise gain a tactical advantage at war.
- Domestic terrorists may break into the private servers of a corporation in order to learn trade secrets, steal banking information, or perhaps the private data of their employees.
- Global terror networks may disrupt a major website, in order to create a public nuisance or inconvenience, or even more seriously, try to stop traffic to a website publishing content with which they disagree.
- International terrorists could try to access and disable the signal which flies drones or otherwise controls military technology.
- A cyber terrorist could try to attack the next generation of air traffic control systems, or collide two large civilian aircraft or try to derail the trains on the rail lines.

1.4.13 Social Engineering Identity Theft

Social engineering identity theft is a method where the cyber criminals make a direct contact with people using emails or phones with the intention to deceive. They try to gain their confidence and once they succeed at it, they get the information they need. This information can be personal, about money, about the company where someone works or anything that can be of interest to the cyber criminals.

It is easy to find out basic information about people from the Internet. Using this information as the base, the cyber criminals try to befriend them and once they succeed, they will disappear, leaving people prone to different financial injuries directly and indirectly. They can sell the information obtained from people or use it to secure things like loans in their name. They use social engineering for Identity theft. So, the people should be very careful when dealing with strangers – both on phone and on the Internet.

1.4.14 Cyber Extortion

Cyber extortion is a crime involving an attack or threat of attack coupled with a demand for money to avert or stop the attack.In such attacks, while cybercriminals threaten to cripple websites or disclose sensitive data, the data itself (stolen or accessed without authorization) is not tampered with and is usually safely returned on demands of the cyber extortionists being met. Simply put, hackers are forcing companies to pay them to desist from impeding commercial operations – a fee to be left alone.

Cyber extortion can take many forms. Originally, denial of service (DoS) attacks against corporate websites were the most common method of cyber extortion; the attacker might initiate a ping storm and telephone the president of the company, demanding that money be wired to a bank account in a foreign country in exchange for stopping the attack.

In a shocking revelation, two Indian companies conceded to having paid hackers money to the tune of $10 million, to protect sensitive information stolen from their compromised computer networks, from imminent exposure. As the stolen information was incriminatory in nature, the attacks which seems to have originated in the Middle East, went unreported by the companies' even months after payments had been made and no case has been filed by either company. Nevertheless, the discovery has prompted an unprecedented interest in understanding cyber extortion, its operation and treatment in India.

In recent years, however, cybercriminals have developed ransomware which encrypts the victim's data. The extortionist's victim typically receives an email that offers the private decryption key in exchange for a monetary payment in Bitcoins, a digital currency. In another instance of cyber extortion, a businessman from Hyderabad recently found himself unable to access his company's database as it had been encrypted by a hacker demanding payment for decryption.

Cyber extortion can be lucrative, netting attackers millions of dollars annually. Unfortunately, as with other types of extortion, payment does not guarantee that further cyber-attacks will not be launched. Most cyber extortion efforts are initiated through malware in e-mail attachments or on compromised websites. To mitigate the risks associated with cyber extortion, experts recommend that end users should be educated about phishing exploits and back up their computing devices on a regular basis.

1.4.15 Intellectual Property Theft

Intellectual property theft involves robbing people or companies of their ideas, inventions, and creative expressions—known as "intellectual property". It includes theft of material that is copyrighted or patented, the theft of trade secrets, and trademark violations.

A copyright is the legal right of an author, publisher, composer, or other person who creates a work to exclusively print, publish, distribute, or perform the work in public. Examples of copyrighted material commonly stolen online are computer software, recorded music, movies, and electronic games.

A patent is an exclusive right granted by a country to the owner of an invention to make, use, manufacture and market the invention, provided the invention satisfies certain conditions stipulated in the law. Exclusive right implies that no one else can make, use, manufacture or market the invention without the consent of the patent holder. This right is available for a limited period of time.

Theft of trade secrets means the theft of ideas, plans, methods, technologies, or any sensitive information from all types of industries including manufacturers, financial service institutions, and the computer industry. Trade secrets are plans for a higher speed computer, designs for a highly fuel-efficient car, a company's manufacturing procedures, or the recipe for a popular salad dressing, cookie mix, or barbeque sauce. These secrets are owned by the company and give it a competitive edge. Theft of trade secrets damages the competitive edge and therefore the economic base of a business.

A trademark is the registered name or identifying symbol of a product that can be used only by the product's owner. Trademarks may be one or a combination of words, letters and numerals. They may also consist of drawings, symbols, three-dimensional signs such as shape and packaging of goods, or colours used as a distinguishing feature. Collective marks are owned by an association whose members use them to identify themselves with a level of quality. Certification marks are given for compliance with defined standards, for example ISO9000.A trademark provides to the owner of the mark by ensuring the exclusive right to use it to identify goods or services or to authorize others to use it in return for some consideration (payment). A trademark violation involves counterfeiting or copying brand name products such as well-known types of shoes, clothing, and electronics equipment and selling them as the genuine or original product.

The two forms of intellectual property most frequently involved in cyber-crime are copyrighted material and trade secrets. Piracy is a term used to describe intellectual property theft—piracy of software, piracy of music, etc. Historically, when there were no computers, intellectual property crimes involved a lot of time and labour. In the twenty-first century software, music, and trade secret pirates operate through the Internet. Anything that can be digitized—reduced to a series of zeroes and ones - can be transmitted rapidly from one computer to another. There is no reduction of quality in second, third, or fourth generation copies. Pirated digital copies of copyrighted work transmitted over the Internet are known as "warez." Warez groups are responsible for illegally copying and distributing hundreds of millions of dollars of copyrighted material.

Pirated trade secrets are sold to other companies or illegal groups. Trade secrets no longer have to be physically stolen from a company. Instead, corporate plans and secrets are downloaded by pirates onto a computer disc. The stolen information can be transmitted worldwide in minutes. Trade secret pirates find pathways into a company's computer systems and download the items to be copied. Companies keep almost everything in their computer files. Pirated copies are sold over the Internet to customers who provide their credit card numbers and then download the copy.

1.4.16 Computer Vandalism

Computer vandalism is a type of mischievous behavior that damages computers and data in various ways and disrupts businesses. Typical computer vandalism involves the creation of malicious programs designed to perform harmful tasks such as extracting login credentials or erasing hard drive data. Cyber vandals are individuals who damage information infrastructures purely for their own enjoyment and pleasure. Their primary motivation is not financial; it is the desire to prove that the feat could be accomplished. Once inside they leave their mark so there is no denying their presence. At first brush this may seem more of a prank than an attack aimed at destruction. The effect on business, however, is undeniable. These types of attacks fall into the category of denial of service attack. The affected site must be shut down and repaired before it can be returned to normal operation.

1.4.17 Computer Viruses and Worms

A virus is a program that searches out other programs and ‘infects’ them by embedding a copy of itself in them. When these programs are executed, the embedded virus is executed too, thus propagating the ‘infection’. This normally happens invisibly to the user.However, unlike a worm, a virus cannot infect other computers without assistance. The virus may do nothing but propagate itself and then allow the program to run normally. Virus spreads to other computers through network file system, through the network, Internet or by the means of removable devices like USB drives and CDs. Usually, however, after propagating silently for a while, it starts doing things like writing messages on the terminal or playing strange tricks with the display. Certain viruses, written by particularly perversely minded crackers, do irreversible damage, like deleting all the user’s files. Computer virusis a form of malicious code written with an aim to harm a computer system and destroy information. Writing computer viruses is a criminal activity as virus infections can crash computer systems, thereby destroying great amounts of critical data.

On the other hand, a worm is a program that propagates itself over a network, reproducing itself as it goes. Therefore, worm, unlike a virus, does not require a medium to propagate itself and infect other computers.

1.4.18 Trojan Horses

Trojan horse is a malicious, security-breaking program that is disguised as something benign, such as a directory lister, archiver, game, or a program to find and destroy viruses. It portrays itself as something other than what it is at the point of execution. The malicious functionality of a Trojan horse may be anything undesirable for a computer user, including data destruction or compromising a system by providing a means for another computer to gain access, thus bypassing normal access controls.

A special case of Trojan horses is the mockingbird — software that intercepts communications (especially login transactions) between users and hosts and provides system-like responses to the users while saving their responses (especially account IDs and passwords).

1.4.19 Logic Bombs

In a computer program, a logic bomb, also called slag code, is programming code, inserted surreptitiously or intentionally, that is designed to execute (or "explode") under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command. It is in effect a delayed-action computer virus or Trojan horse. A logic bomb, when "exploded," may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects.

Some logic bombs can be detected and eliminated before they execute through a periodic scan of all computer files, including compressed files, with an up-to-date anti-virus program. For best results, the auto-protect and e-mail screening functions of the anti-virus program should be activated by the computer user whenever the machine is online. In a network, each computer should be individually protected, in addition to whatever protection is provided by the network administrator. Unfortunately, even this precaution does not guarantee 100-percent system immunity.

In an instance of logic bomb, a computer systems administrator for UBS PaineWebber was charged with using a ‘logic bomb’ to cause more than $3 million in damage to the company’s computer network. It was alleged that from November 2001 to February 2002, the accused constructed the logic bomb computer program. On March 4, as planned, his program activated and began deleting files on over 1,000 of PaineWebber’s computers [U.S. v Smith]6.

1.4.20 Back Door

It is also called trap door. It is another way to enter into a computer is by creating a back door. It is a hole in the system’s security deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor’s maintenance programmers. Historically, back doors have often lurked in systems longer than anyone expected or planned, and a few have become widely known.

1.4.21 Malvertising

Malvertising is a method whereby users download malicious code by simply clicking at some advertisement on any website that is infected. In most cases, the websites are innocent. It is the cyber criminals who insert malicious advertisements on the websites without the knowledge of the latter. It is the work of advert companies to check out if an advertisement is malicious but given the number of advertisements they have to deal with, the malverts easily pass off as genuine ads.

In other cases, the cyber criminals show clean ads for a period of time and then replace it with malverts so that the websites and advertisements do not suspect. They display the malverts for a while and remove it from the site after meeting their targets. All this is so fast that the website does not even know they were used as a tool for cybercrime. Malvertising is one of the fastest, increasing types of cybercrime.

1.4.22 Hacking

The activity of breaking into a computer system to gain an unauthorized access is known as hacking. It is the act of defeating the security capabilities of a computer system in order to obtain an illegal access to the information stored on the computer system. The unauthorized revelation of passwords with intent to gain an unauthorized access to the private communication of an organization of a user is one of the widely known computer crimes. Another highly dangerous computer crime is the hacking of IP addresses in order to transact with a false identity, thus remaining anonymous while carrying out the criminal activities.

1.4.23 Theft of Internet Hours

Theft of Internet hours refers to using up or utilizing of somebody else’s Internet services. In many cases, when a person takes up the services of any Internet service provider, he utilizes the services in terms of number of hours consumed and makes the payment on a per hour basis. However, in case a third person is able to identify the username and password of the Internet service user, he can easily consume those Internet hours.

1.4.24 Salami Attacks

This attack is used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed, e.g. a bank employee inserts a program into the bank’s servers, which deducts a small amount of money (say 10 paisa a month) from the account of every customer. No single account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month. The classic story about a salami attack is the old “collect-the-round off” trick. In this scam, a programmer modifies arithmetic routines, such as interest computations. Typically, the calculations are carried out to several decimal places beyond the customary two or three kept for financial records. For example, when currency is in rupees, the round off goes up to the nearest paisa about half the time and down the rest of the time. If a programmer arranges to collect these fractions of paisa in a separate account, a sizable fund can grow with no warning to the financial institution.

1.4.25 Data Diddling

This computer crime relates to operation security and is minimized through strengthening of internal security controls. This kind of an attack involves altering the raw data just before it is processed by a computer and then changing it back after the processing is completed. This is a simple and common computer related crime which involves changing data prior to or during input to a computer. Data can be changed by anyone involved in the process of creating, recording, encoding, examining, checking, converting, or transporting computer data.

1.4.26 Steganography

Steganography is the process of hiding one message or file inside another message or file. It is “the art of writing in cipher, or in characters, which are not intelligible except to persons who have the key”. It has been used in ancient times as well. In computer terms, steganography has evolved into the practice of hiding a message within a larger one in such a way that others cannot discern the presence or contents of the hidden message. In contemporary terms, steganography has evolved into a digital strategy of hiding a file. For instance, steganographers can hide an image inside another image, an audio file, or a video file, or they can hide an audio or video file inside another media file or even inside a large graphic file. Steganography differs from cryptography in that while cryptography works to mask the content of a message, steganography works to mask the very existence of the message.

Following steps are generally followed to achieve the desired result:

(a) Locating a data/video/audio file which requires being hidden and transmitted.

(b) Locating a carrier file which will carry the data/video/audio file.

(c) Using appropriate steganography software which will permit embedding of the data/video/audio file into the carrier file and at the receiver’s end, permit extraction thereof. A few softwares even permit password protection.

(d) E-mailing the carrier file to the receiver.

(e) Decryption of the message by the receiver.

There have been reports of Osama bin Laden and others hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites.

1.4.27 Cyber Warfare

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks. Cyberwarfare is Internet-based conflict involving politically motivated attacks on information and information systems. Cyberwarfare attacks can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems -- among many other possibilities.

Any country can wage cyberwar on any other country, irrespective of resources, because most military forces are network-centric and connected to the Internet, which is not secure. For the same reason, non-governmental groups and individuals could also launch cyberwarfare attacks.

Examples of cyber warfare include:

- In 1998, the United States hacked into Serbia's air defence system to compromise air traffic control and facilitate the bombing of Serbian targets.
- In 2007, in Estonia, a botnet of over a million computers brought down government, business and media websites across the country. The attack was suspected to have originated in Russia, motivated by political tension between the two countries.
- Also in 2007, an unknown foreign party hacked into high tech and military agencies in the United States and downloaded terabytes of information.
- In 2009, a cyber spy network called "GhostNet" accessed confidential information belonging to both governmental and private organizations in over 100 countries around the world. GhostNet was reported to originate in China, although that country denied responsibility.

The most effective protection against cyberwarfare attacks is securing information and networks. Security updates should be applied to all systems -- including those that are not considered critical -- because any vulnerable system can be co-opted and used to carry out attacks. Measures to mitigate the potential damage of an attack include comprehensive disaster recovery planning that includes provisions for extended outages.

1.5 CYBER FORENSICS

Cyber forensics (or computer forensics) is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Forensic investigators typically follow a standard set of procedures. After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.

The need or the importance of the computer forensics is to ensure the integrity of the computer system. The system with some small measures can avoid the cost of operating and maintaining the security. The subject provides in depth knowledge for the understanding of the legal as well as the technical aspects of computer crime. It is very much useful from a technical stand point, view.

The importance of computer forensics is evident in tracking the cases of the child pornography and email spamming. The computer forensics has been efficiently used to track down the terrorists from the various parts of the world. The terrorists using the internet as the medium of communication can be tracked down and their plans can be known.

There are many tools that can be used in combination with the computer forensics to find out the geographical information and the hide outs of the criminals. The IP address plays an important role to find out the geographical position of the terrorists. The security personnel deploy the effective measures using the computer forensics. The Intrusion Detecting Systems are used for that purpose.

A number of techniques are used during computer forensics investigations such as:

- **Cross-drive analysis** – It is a forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection.
- **Live analysis** – It involves examination of computers from within the operating system using custom forensics or existing system administration tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.
- **Deleted files** – It is a common technique used in computer forensics to recover the deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.
- **Stochastic forensics** – It is a method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.
- **Steganography** – It is one of the techniques used to hide data via steganography. It involves the process of hiding data inside of a picture or digital image. An

example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available). While the image appears exactly the same, the hash changes as the data changes.

1.6 SUMMARY

Computer crime is a growing threat to society caused by the criminals and irresponsible actions of individuals who are taking advantage of the widespread use of computer networks in our society. It presents a major challenge to the ethical use of information technologies. Computer crime poses serious threats to the integrity, safety, and survival of most e-business systems, and thus makes the development of effective security methods a top priority. According to Association of Information Technology Professionals (AITP), computer crime includes The unauthorized use, access, modification, and destruction of hardware, software, data, or network resources. The unauthorized release of information. The unauthorized copying of software. Denying an end user access to his or her own hardware, software, data, or network resources. Using or conspiring to use computer or network resources to illegally obtain information or tangible property. Cyber-crime encompasses any criminal act dealing with computers and networks (called hacking). Cyber-crime includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber-crimes when the illegal activities are committed through the use of a computer and the Internet. Cyber-crimes also includes offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).Cyber-crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyberwarfare. The international legal system is attempting to hold actors accountable for their actions through the International Criminal Court. Computer crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are subject everywhere to criminal sanctions. The term computer misuse and abuse are also used frequently but they have significantly different implications. Annoying behavior must be distinguished from criminal behavior in Law.

1.7 EXERCISE

Exercise 1 : Mix and Match

– It involves examination of computers from within the operating system using custom forensics or existing system administration tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.	**Deleted files**
– It is a common technique used in computer forensics to recover the deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.	**Live analysis**
– It is a method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.	**Steganography**
– It is one of the techniques used to hide data via steganography. It involves the process of hiding data inside of a picture or digital image.	**Stochastic forensics**

Ans 1 (2), 2(1), 3(4), 4(3)

Exercise 2: Fill in the Blanks

(a) Locating a data/video/audio file which requires being…………………..

(b) ……………..carrier file which will carry the data/video/audio file.

(c) Using appropriate ………………….which will permit embedding of the data/video/audio file into the carrier file and at the receiver's end, permit extraction thereof. A few softwares even permit password protection.

(d) …………………..the carrier file to the receiver.

Ans. 1. hidden and transmitted 2. Locating a 3. Steganography software 4. E-mailing

Exercise 3: True / False

(a) Cyber-crime encompasses any criminal act not dealing with computers and networks (called hacking).

(b) Cyber-crime does not includes traditional crimes conducted through the Internet.

(c) Cyber forensics (or computer forensics) is not the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.

(d) It is not a method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.

Ans . 1. False 2. False 3. False 4. False

Exercise 4: Question Answers

1. What do you understand by Cyber crimes?

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

2. Differentiate between Computer Crime and Cyber Crime.

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

3. Distinction between cyber crime and conventional crimes;

………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………
………………………………………………………………………………………

4. Explain various Kinds of cyber crimes

   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………

5. Explain cyber stalking, cyber terrorism, forgery and fraud, cyber forensic

   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………
   ……………………………………………………………………………………

Unit II

DEFINITIONS UNDER IT ACT, 2000

- Definitions under IT Act, 2000;
- Concept of Internet,
- Web Centric Business,
- E Business and its significance,
- Electronic Governance,
- Cyber jurisdiction
- Summary
- Exercise

2.1 DEFINITIONS UNDER IT ACT, 2000

The Indian Parliament has enacted an Act called the Information Technology Act, 2000 (ITA 2000). The Information Technology (Amendment) Act, 2008 (ITAA 2008) is a substantial addition to India's ITA 2000. Section 2(1) of ITA 2000 gives the definitions of key terms. Some changes have been made to the definitions by the ITAA 2008. The word “digital signature” was substituted by “electronic signature”. It should be noted that digital signature is a sub set of electronic signature. The ITAA 2008 in order to maintain continuity with the regime of the digital signature has introduced the concept of ‘electronic signature’. Examples of electronic signatures may include biometric signatures, passwords, PINs, encryption applications etc.

The updated definitions are given as under:

(a) **“Access”**, with the grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network;

(b) **“Addressee”** means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(c) **“Adjudicating Officer”** means an adjudicating officer appointed under sub-section (1) of Section 46;

(d) **“Affixing Electronic Signature”** with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic signature;

(e) **“Appropriate Government”** means as respects any matter-

   (i) Enumerated in List II of the 7th Schedule to the Constitution;

   (ii) Relating to any State Law enacted under List III of the 7th schedule to the Constitution, the State Government and in any other case, the Central Government;

(f) **“Asymmetric Crypto System”** means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) **“Certifying Authority”** means a person who has been granted a license to issue an Electronic Signature Certificate under Section 24;

(h) **“Certification Practice Statement”** means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Electronic Signature Certificates;

(ha) **"Communication Device"** means Cell Phones, Personal Digital Assistance (Sic), or combination of both or any other device used to communicate, send or transmit any text, video, audio, or image. (Inserted Vide ITAA 2008)

(i) **“Computer”** means any electronic, magnetic optical or other high-speed data processing device or system which performs logical arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;

(j) (Substituted vide ITAA 2008)

(i) **‘Computer Network’** means the interconnection of one or more computes through-

(ii) The use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(iii)Terminal or complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

(k) **“Computer Resource”** means computer, computer system, computer network, data, computer database or software;

(l) **“Computer System”** means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(m)**“Controller”** means the Controller of Certifying Authorities appointed under sub-section (1) of section 17;

(n) **“Cyber Appellate Tribunal”** means the Cyber Appellate Tribunal established under sub-section (1) of section 48;

(na) (Inserted Vide ITAA 2008)

“Cyber Café” means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public.

(nb) (Inserted Vide ITAA 2008)

"Cyber Security" means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

(o) **“Data”** means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

(p) **“Digital Signature”** means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

(q) **“Digital Signature Certificate”** means a Digital Signature Certificate issued under sub-section (4) of section 35;

(r) “**Electronic Form”** with reference to information, means any information generated sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

(s) **“Electronic Gazette”** means the Official Gazette published in the electronic form;

(t) **“Electronic Record”** means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

(ta) (Inserted Vide ITAA 2008)

“Electronic Signature” means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature;

(tb) (Inserted Vide ITAA 2008)

“Electronic Signature Certificate” means an Electronic Signature Certificate issued under Section 35 and includes Digital Signature Certificate;

(u) **“Function”** in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

(ua) “Indian Computer Emergency Response Team” means an agency established under sub-section(1) of section 70B;

(v) **“Information”** includes data, message, text, images, sound, vice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche; (Substituted vide ITAA 2008)

(w) (Substituted vide ITAA 2008)

“Intermediary” with respect to any particular electronic message, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;

(x) **“Key Pair”** in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

(y) **“Law”** includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be, Regulations made by the President under Article 240, Bills enacted as President’s Act under sub-clause (a) of clause (1) of Article 357 of the Constitution and includes rules, regulations, by-laws and orders issued or made there under;

(z) **“License”** means a license granted to a Certifying Authority under Section 24;

(za) **“Originator”** means a person who sends, generates, stores or transmits any electronic message; or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

(zb) **“Prescribed”** means prescribed by rules made under this Act;

(zc) **“Private Key”** means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

(zd) **“Public Key”** means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificates;

(ze) **“Secure System”** means computer hardware, software, and procedure that-

(a) Are reasonably secure from unauthorized access and misuse;

(b) Provide a reasonable level of reliability and correct operation;

(c) Are reasonably suited to performing the intended functions; and

(d) Adhere to generally accepted security procedures;

(zf) **“Security Procedure”** means the security procedure prescribed under Section 16 by the Central Government;

(zg) **“Subscriber”** means a person in whose name the Digital Signature Certificate is issued;

(zh) **“Verify”** in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions, means to determine whether-

(a) The initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;

(b) The initial electronic record is retained in act has been altered since such electronic record was so affixed with the digital signature.

2.2 CONCEPT OF INTERNET

Internet is the backbone of rapid growth of technological revolution. The word Internet is derived from Internetworking that is a collection of individual networks, connected by intermediate networking devices that function as a single large network. Network is a collection of terminals, computer servers and components which allow for the easy flow of data and use of resources between one another. In simple words, a network is a group of two or more computer systems linked together. Internet is a global communication network. It is also called network of networks.

Millions of computers all over the world are connected through the Internet. Computer users on the Internet can contact one another anywhere in the world. If your computer is connected to the Internet, you can connect to millions of computers. You can gather information, distribute data and share resources.

Internet enables a huge amount of information to people across the world. It provides many computer-based facilities such as E-mail, Electronic Data Interchange, Information Publishing, Information retrieval etc. Information in every field starting from education, science, health, medicine, history, and geography to business, news etc can be retrieved through Internet. You can also download programs and software packages from anywhere in the world. Due to the tremendous information resources the Internet can provide, it is now indispensable to every organization.

There are 4 main ways to connect to the Internet. These methods include connecting via a LAN server, connecting via SLIP/PPP, connecting via an online service, or connect through broadband. They are explained below:

- **Connect via LAN Server:** This approach needs the user's computer to have specific protocol "Example IP" with specific configuration, which provides a set of communications rules that perform the complete functions of the seven layers of the OSI communication model. LAN servers are typically connected to the internet at 2Mbps or faster. This type of connection is expensive, but cost can be spread over multiple LAN users.
- **Connect via Serial Line Internet Protocol/Point-to-point Protocol (SLIP/PPP):** This approach needs that the users have modem and specialized software that allows them to dial into a server through a service provider at some specific cost. This type of connection is advantageous, for example, for employees working at home who need to access the Internet or their own Intranet.
- **Connect via an Online Service:** This approach needs a modem, standard communication software and an online information service account with an Internet service provider. The cost includes the online service fee, per-hour connect charge and where applicable, e-mail service charges. There are so many service providers throughout India like Airtel, Vodafone, Idea Cellular, Reliance Communications, BSNL, Aircel, Tata Teleservices, Telenor India, MTNL, Videocon etc.
- **Connect through Broadband:** This type of connection is very popular right now because here the data transfer speed is more than 256 KBPS without interruption. In India, almost all Internet Service Providers (ISP) provides Broadband connection with a very nominal cost.

2.3 WEB CENTRIC BUSINESS

Large number of companies adopting this technique to curb the existing inefficiencies involved in potentially time consuming and tedious tasks, while cutting down the costs. It links suppliers, factories, distributors, and retailers directly.

It allows the business to replace number of people in their works department with automated systemsvIt substantially reduces business cycle time. vIt helps in running the business more efficiently, quickly and securely.vManaging inventory more efficientlyvAdjusting more quickly to customer demandvGetting products to market fasterνCutting the cost of paperworkνReigning in rogue purchasesνObtaining lower prices on some supplies.

To transform the scenario of the business, there are various models of e-commerce,which are being proposed to establish an electronic link between the business and consumers.These models have brought business and consumer closer to each other & transformed theway of conducting the business drastically. Business models are being classified as following:

Business to Consumer (B2C)

Business to Business (B2B)

Consumer-to-Consumer or Peer-to-Peer (C2C/P2P)

Consumer-to-Business (C2B)

Business to Government (B2G)

2.4 E BUSINESS AND ITS SIGNIFICANCE

E-Business involves changes in an organizations business and functional processes with the application of technologies, philosophies and computing paradigms of the new digital economy. It is an interent initiative which transforms business relationship. It includes all aspects of e-commerce. With the help of e-business solutions, the companies have succeeded in developing their technology and increasing their turnover. To gether e-business and E-commerce have helped create a systems of applications andutilities whereby money, information and services can be exchanged via the web. It is important tto align the main business of the firm the e-business strategy of the firm in order to succeed.

2.5 ELECTRONIC GOVERNANCE

In 2005, the UN-sponsored World Summit on the Information Society defined Internet governance as "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet". Many information policy experts emphasize that "Internet governance" is not the product of an institutional hierarchy, but rather, it emerges from the decentralized, bottom-up coordination of tens of thousands of mostly private-sector entities across the globe. Often referred to as Internet "stakeholders," these include network and server operators, domain name registrars and registries, IP address and standards organizations, Internet service providers, and individual users. Civil society organizations and governments participate alongside these stakeholders in contributing to the development of technical policies.

Internet governance has the following characteristics:

- It consists of evolving policies and mechanisms under which the Internet community's many stakeholders make decisions about the development and use of the Internet.
- It consists of the collective rules, procedures, processes, and related programs that shape social actors', shared expectations, practices, and interactions and result in practices and operations that are consistent with the sovereign rights of states and the social and market interests of end-users and operators.

- It includes agreements about standards, policies, rules, and enforcement and dispute resolution procedures.
- It is not limited to technical issues only. It includes important social, economic, and national security issues. It covers wide range of issues, from day-to-day technical and operational workings of the Internet to public policy issues such as combating crime on the Internet.
- States control Internet-related policies within their own borders, such as passing laws prohibiting online gambling, protecting intellectual property, or blocking/filtering access to certain content.

No one person, company, organization or government runs the Internet. It is a globally distributed network comprising many voluntarily interconnected autonomous networks. It operates without a central governing body with each constituent network setting and enforcing its own policies. Its governance is conducted by a decentralized and international multi-stakeholder network of interconnected autonomous groups drawing from civil society, the private sector, governments, the academic and research communities and national and international organizations. They work cooperatively from their respective roles to create shared policies and standards that maintain the Internet's global interoperability for the public good.

However, there are certain bodies that looks after different aspects of internet governance. They are described below:

- **Internet Corporation for Assigned Names and Numbers (ICANN)** – It is a private sector, non-profit organization created in 1988 under contract to the U.S. Department of Commerce. It coordinates the Domain Name System (DNS), Internet Protocol (IP) addresses, space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. It seeks to create a globally unified namespace to ensure the global reach of the Internet. It has no control over the content and doesn’t deal with access to the internet. It helps co-coordinate the supply and assignment of IP addresses to help stop duplicate IP address problems. It is governed by an international board of directors drawn from across the Internet's technical, business, academic, and other non-commercial communities. However, the National Telecommunications and Information Administration, an agency of the U.S. Department of Commerce, continues to have final approval over changes to the DNS root zone.
- **Internet Assigned Numbers Authority (IANA)** – It is a department of ICANN. It is responsible for the global coordination of the DNS Root, the .int and .arpa domains, IP addressing, and other Internet protocol resources such as IP numbers or addresses. IANA manages the global pool of Internet numbers (Internet Protocols IPs and Autonomous System Numbers ASNs) and distributes them among the five regional Internet registries (RIRs).
- **Internet Engineering Task Force (IETF)** – It is a non-profit organization of loosely affiliated international participants that anyone may associate with by contributing technical expertise. It started out as an activity supported by the U.S. federal government, but since 1993 it has operated as a standards development

function under the auspices of the Internet Society (ISOC), an international membership-based non-profit organization. It develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP). It produces high quality, relevant technical documents that influence the way people design, use, and manage the Internet. The technical underpinning and standardization of the Internet's core protocols (IPv4 and IPv6) is an activity of the IETF.

- **Internet Society (ISOC)** – It is an American, non-profit organization founded in 1992 to provide leadership in Internet-related standards, education, access, and policy. It aims to promote the open development, evolution and use of the Internet for the benefit of all people throughout the world. It handles development, maintenance, evolution, and dissemination of standards for the Internet and its internet working technologies and applications.
- **Internet Architecture Board (IAB)** - It is a committee of the Internet Engineering Task Force (IETF) and an advisory body of the Internet Society (ISOC). Its responsibilities include architectural oversight of IETF activities, Internet Standards process oversight and appeal, and the appointment of the Request for Comments (RFC) Editor. The IAB is also responsible for the management of the IETF protocol parameter registries. It focus is in making the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. Some of examples of recent IAB dealings include the future of Internet addressing, partial checksums for UDP traffic, network management, and service identifiers and filtering.
- **World Wide Web Consortium (W3C)** – It is the main international standards organization for the World Wide Web (abbreviated WWW or W3). In October of 1994, Tim Berners-Lee, the inventor of the WWW founded it at MIT. W3C works mostly on the standardization of Web Technologies. To help come up with the highest quality of standards, W3C uses a community consensus. All the stakeholders involved do have an opportunity to have a voice in the development of W3C standards. After the technical report development process is complete, W3C publishes recommendations. There recommendations considered web standards. It is up to manufacturers to follow the recommendations of W3C. If a product would like to be labeled W3C-compliant, it must meet the defined level of conformance set by the W3C. Before W3C was created there were different versions of HTML put out on the market by various vendors. Many of these different versions were not compatible with each other. The consortium allowed the vendors to get together and agree on core principles which everyone would use. Some web standards that W3C is responsible for are: CSS, XHTML, HTML, XML, P3P, and OWL. The W3C also engages in education and outreach, develops software and serves as an open forum for discussion about the Web. W3C is working on device independence as well. Device independence would allow the web to be accessible by any device under any circumstance.
- **International Standards Organization (ISO)** - It is an international standard-setting body composed of representatives from various national standards organizations. Founded on 23 February 1947, ISO promotes worldwide proprietary,

industrial and commercial standards. It is headquartered in Geneva, Switzerland, and works in 162 countries. It has developed standards that apply to the governance of management processes (and decisions) relating to the information and communication services used by an organization. It is the world's largest developer of voluntary international standards and facilitates world trade by providing common standards between nations. Nearly twenty thousand standards have been set covering everything from manufactured products and technology to food safety, agriculture and healthcare.

- **Institute for Electrical and Electronics Engineers (IEEE)** - IEEE was formed in 1963 from the amalgamation of the American Institute of Electrical Engineers and the Institute of Radio Engineers. Today, it is the world's largest association of technical professionals with more than 400,000 members in chapters around the world. Its objectives are the educational and technical advancement of electrical and electronic engineering, telecommunications, computer engineering and allied disciplines. The IEEE has played a large and important role in the ongoing realm of internet governance. The group is responsible for such standards as the 802.3 Ethernet and the 802.11 wireless networking standards. Both of these standards are heavily used access standards for the Internet and can be considered among the IEEE’s most important standards today. The IEE continues to push development and innovation standards in the power and energy, information technology, and telecommunications fields with over 1300 standards in development. One of IEEE’s most recent developments is the ratification of the 802.11n wireless networking standard which brings increased range and data rates for wireless data transmission.
- **International Telecommunications Union (ITU)** - It is a specialized agency that is responsible for issues that concern information and communication technologies. In 1947, it became a specialized agency of the United Nations (UN). It aims to enable the growth and sustained development of telecommunications and information networks, and to facilitate universal access so that people everywhere can participate in, and benefit from, the emerging information society and global economy. ITU has participated in improving the level of connectivity on a global scale. ITU has participated at the physical level by improving the global telecommunications infrastructure. It has made efforts from a governance and policy perspective by establishing global standards for communications systems. It continues to look ahead and address new issues to telecommunications and networking by helping to strengthen cyber security. It coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world, and assists in the development and coordination of worldwide technical standards. The ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks.
- **International Electro-technical Commission (IEC)** - It is a non-profit, non-governmental international standards organization that prepares and publishes

International Standards for all electrical, electronic and related technologies – collectively known as electro-technology. IEC standards cover a vast range of technologies from power generation, transmission and distribution to home appliances and office equipment, semiconductors, fiber optics, batteries, solar energy, nanotechnology and marine energy as well as many others. The IEC also manages three global conformity assessment systems that certify whether equipment, system or components conform to its International Standards.

2.6 CYBER JURISDICTION

Jurisdiction means the authority which a court has to decide matters that are litigated before it or to take cognizance if matters are presented in a formal way for its decisions. Jurisdiction could be said that it is the power / authority of the court to decide matters that are brought before him. In this context, jurisdiction over activities on the Internet has become a battleground for the struggle to establish Rule of Law in the Information Society. The rise of the global computer network is destroying the link between geographical location and:

- The power of local governments to assert control over online behavior;
- The effects of online behavior on individuals or things;
- The legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and
- The ability of physical location to give notice of which sets of rules to apply.

The internet thus radically subverts a system of rule-making based on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territorially defined rules.

The Internet explosion has generated many jurisdictional disputes, putting the onus on courts to determine how to apply historic concepts regarding personal jurisdiction to the boundary-less world of the Internet. With so many outsourcing activities in India and the popularity of networking websites, a fresh continuum of cases related to “Personal Victimization” and “Economic Offences” in the nature of data protection, cyber defamation, security, etc have evolved. Hacking initiated at one place adversely affects any other place/institution and brings them to limbo.

There is an ongoing debate over the jurisdiction of Indian Courts in combating cyber-crimes, committed by outsider effecting Indian cyber space located in India. For example, Website offering pornographic materials has set up its server in America, in which there is no ban on selling obscene material above legal age, whose owner resides in France and the customer from India buys some material from the same, which prohibits such transmission and distribution of such material. Here the question arises where the transaction has taken and who is liable. The continuous outreach of Internet has made it difficult to limit the use pornography; it has even reached to the hands of children‘s on a large scale. Indian Police finds itself in a dilemma, how to arrest the person, located outside India. Child pornography is not prohibited in many countries.

2.6.1 Legal Provisions Related to Cyber Jurisdiction

The relevant legislations relating to cyber jurisdiction in India are:

- Information Technology Act, 2000 - Section 75 of the Act implies that the Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence involves a computer, computer system or computer network located in India.
- Indian Penal Code, 1860 - Section 3 and 4 of the Act deals with the extra-jurisdictional power given to the Indian Courts.
- Code of Criminal Procedure, 1973 - Section 188 provides that even if a citizen of India outside the country commits the offence, the same is subject to the jurisdiction of courts in India. In India, jurisdiction in cyberspace is similar to jurisdiction as that relating to traditional crimes and the concept of subjective territoriality will prevail. Moreover Section 178 deals with the crime or part of it committed in India and Section 179 deals with the consequences of crime in Indian Territory.

2.6.2 Role Played by Indian Courts Regarding Cyber Jurisdiction

In a leading case of cyber-crime, SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra, India’s first case of cyber defamation, High Court of Delhi assumed jurisdiction over a matter where a corporate’s reputation was being defamed through e-mails, and passed an important ex-parte injunction. The concept of consequence and cause of action extends jurisdiction but a conflicting situation arises where there is no defined regulation at one of the places. For example, the Act does not provide any provision to catch the internet pornography on foreign websites but only for sites in India.

The Supreme Court of India, in the case of SIL Import v. Exim Aides Silk Importers has recognized the need of the judiciary to interpret a statute by making allowances for any relevant technological change that has occurred. Until there is specific legislation in regard to the jurisdiction of the Indian Courts with respect to Internet disputes, or unless India is a signatory to an International Treaty under which the jurisdiction of the national courts and the circumstances under which they can be exercised are spelt out, the Indian Courts will have to give a wide interpretation to the existing statutes, for exercising Internet disputes.

2.6.3 Need of the Hour for India Regarding Cyber Jurisdiction

In the present scenario where the cyber-crimes are increasing to an alarming extent, the present need of the hour is to have broad based convention dealing with criminal substantive law matters, criminal procedural questions as well as with international criminal law procedures and agreements. The IT Act, 2000 would be crippled without proper means and ways of implementing it. To overcome the difficulties, necessary amendments must be made to The Code of Criminal Procedure, 1973. Moreover, it is important to note that India at present does not have a proper extradition law to deal with crimes that have been committed over the Internet. To address this issue, India should become a signatory to the Convention of cyber-crimes treaty and should ratify it. This move would go a great deal in resolving the jurisdictional controversies that may arise in cyber-crime cases.

2.6.4 P2P Networks and Copyright Industry

Millions of people around the world have downloaded various P2P software and are increasingly using them to exchange music, movie and software files. The copyright industry has been giving figures that go to show the decline in the sales of copyrighted products and they cite the reason as Internet piracy. The stakes as reported by the Industry are definitely high. The Industry points the finger directly at the Internet. The industry argues that online piracy eliminates the economic incentives for a business to invest millions in the production of movies, software, video games, CD's, etc. A business will no longer get a return on its investment if a consumer can just get it for free online. In that manner Internet piracy would hinder the growth of creativity.

Shocked and dismayed, the industry in the last couple of years has been fighting this menace of 'piracy' on all possible fronts, which include, lobbying, litigation, legislation and technological measures. The industry is starting to prosecute not only companies like Napster but also individuals who download copyrighted content and the persons who make it possible namely the Internet service providers.

In the past, there has been pressure from the industry for stronger protection of their rights in the digital context. In 1996, two treaties were concluded at WIPO: the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) (commonly referred to as the "Internet treaties"). These treaties address the issues of the definition and scope of rights in the digital environment, and some of the challenges of online enforcement and licensing. As a continuation of this process, in many countries laws have emerged in this direction. The industry is continuously looking towards a solution through the courts. But in some litigations, the results have not been very encouraging for the industry.

A pragmatic answer to these problems was provided by the technology itself and the audiovisual industry is currently looking at technological solutions to prevent unauthorized access to or use of copyrighted material, or illicit dissemination of protected works. Technological protections could take many forms and serve many related purposes. Some of these protections are scrambling signals, encryption, passwords, electronic watermark, digital code and the like. By these the product can be locked behind technological barriers – requiring authorization and payment through electronic means before they could be opened up or set aside. The idea is to stop copying in the first place rather than fighting back after it has been done. No matter how sophisticated the technological protections employed, none are invulnerable, and surely smart people will increasingly make it their business to hack through encryption, pick digital locks, steam open electronic envelopes, or obliterate digital watermarks. Since every kind of technical protection provokes circumvention, technical identification and control mechanisms have been backed by accompanying legal protection. In order to protect against the circumvention of technological protections applied to copyrighted products in the digital environment, provisions have been incorporated in the WCT and WPPT making it obligatory for member states to provide legal protection against the circumvention of technological measures.

2.7 SUMMARY

The Indian Parliament has enacted an Act called the Information Technology Act, 2000 (ITA 2000). The Information Technology (Amendment) Act, 2008 is a substantial addition to India's ITA 2000. Section 2(1) of ITA 2000 gives the definitions of key terms. Some changes have been made to the definitions by the ITAA 2008. The word "digital signature" was substituted by "electronic signature". Often referred to as Internet "stakeholders," these include network and server operators, domain name registrars and registries, IP address and standards organizations, Internet service providers, and individual users. Civil society organizations and governments participate alongside these stakeholders in contributing to the development of technical policies.

2.8 EXERCISE

Exercise 1: Mix and Match

with the grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network;	**Addressee**
means a person who is intended by the originator to receive the electronic record but does not include any intermediary;	**Access**
means an adjudicating officer appointed under sub-section (1) of Section 46;	**Affixing Electronic Signature**
with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic signature;	**Adjudicating Officer**

Ans. 1(2), 2 (1), 3(4), 4(3)

Exercise 2: Fill in the blanks

(a) The power of local governments to assert control over online …………..
(b) The effects of online behaviour on…………………. or things;
(c) The legitimacy of the efforts of a local to enforce rules applicable to global phenomena
(d) The ability of physical location to give notice of which sets of ……………...

Ans 1. Behavior 2. Individuals 3. sovereign 4. rules to apply

Exercise 3: True and False

(a) It does not consists of evolving policies and mechanisms under which the Internet community’s many stakeholders make decisions about the development and use of the Internet.
(b) It consists of the collective rules, procedures, processes, and related programs that shape social actors’, shared expectations, practices, and interactions and result in practices and operations that are consistent with the sovereign rights of states and the social and market interests of end-users and operators.

(c) It includes agreements about standards, policies, rules, and enforcement and dispute resolution procedures.

(d) It is limited to technical issues only. It includes important social, economic, and national security issues. It covers wide range of issues, from day-to-day technical and operational workings of the Internet to public policy issues such as combating crime on the Internet.

Ans. 1. False 2. True 3. True 4. False

Exercise 4: Short Question Answers

(a) Explain Definitions under IT Act, 2000

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

(b) Explain the Concept of Internet

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

(c) What is Web Centric Business?

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

(d) Define E Business and its significance

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

(e) Define Electronic Governance

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

(f) Explain Cyber jurisdiction

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

Unit III

CONTEMPORARY BUSINESS ISSUES IN CYBER SPACE

- Security risks:
- Instant messaging platform,
- Social networking sites,
- Nobile applications and Internet of Things (IOT)
- Domain name dispute and their resolution,
- E-forms;
- EMoney,
- Regulations of PPI (Pre-Payment Instruments) by RBI,
- Electronic Money Transfer,
- Privacy of Data and Secure Ways of Operation in Cyber Space

3.1 SECURITY RISK

Security: These security risks can be grouped into three general categories:
(i) Client/Server Risks
(ii) Data transfer and transaction risk
(iii) Virus risk.

3.2 INSTANT MESSAGING PLATFORM

This type of messaging is used for business, education and spreading information. There are many platforms of Instant Messaging Platform (IMPs).
There are many popular IMPs namely as Whats app, skype, facebook messager, viber etc.
Some of the popular Indian IMPs are:
1. Troop
2. Namaste Bharat
3. Telegram
4. Hike
5. JioChat is Indian high secure IMPs shown in figure given below

Social Networking Sites

3.3 SOCIAL MEDIA MARKETING

A process of optimizing your site/blog to be more visible in social media searches and sites, more easily linked by other sites, and more frequently discussed online in blog posts and

other social media

Social Media Marketing uses podcasts, wikis, blogs, online videos, photo sharing, news sharing, message boards and posts on social networking sites to reach a large or targeted audience. shown in figure below:

Some to examples of Social Media Optimization/Marketing Techniques are as follows:

- Joining relevant online communities or social networking sites to help promote your business.
- Adding RSS feeds to your website (RSS stands for Really Simple Syndication that can be used to easily update content).
- Blogging (where you add content to blogs).
- Creating your own business blog.

What is the Difference between SMM (Social Media Marketing) and SMO (Social Media

Optimization)?

Social Media Optimization involves creating the right type of content and building a

site —that is easy to share on social networks and is friendly to social media users whereas

Social Media Marketing goes a step further in terms of actually promoting the content on these

networks and spreading the word about your content.

Why Social Media Optimization/Marketing?

1. One can reach a large number of people in a more spontaneous way without paying large advertising fees.
2. The use of blogs and social and business networking sites can increase traffic to your website from other social media websites. This in turn may increase your Page Rank, resulting in increased traffic from leading search engines.
3. Social media complements other marketing strategies such as <I paid advertising campaign.
4. You can build credibility by participating in relevant forums and responding to questions.

5. Social media sites have information such as user profile data, which can be used to target a specific set of users for advertising.

Tools for Social Media Marketing

1. Wikis (e.g., TWiki, wetpaint, Wikipcdia)
2. Business Networking (e.g., LinkedIn, XINg cAcadcmy)
3. Blogs (e.g., Mashable!, Boing Boing, Dosh Dosh)
4. Social Bookmarking or Tagging (e.g., Digg, Reddit del.icio.us)
5. Collaborative Tools (e.g., Zimbra, zoho, Goolge)
6. Social Networking (e.g., Facebook. Myspace, Friendster)
7. Video Sharing (e.g., YouTube, Kyte)
8. Photo Sharing (e.g., Filckr, zoom, smugmug)
9. Audio Sharing (e.g., Blog Talk Radio, ODLO)

3.4 GOALS AND OBJECTIVES OF SMM

Goals are general, wider intentions whereas objectives are precise, measurable steps that help you to achieve your goals. Identifying your objectives for social media is essential.

If you have no specific reasons for using it, you'll spend a lot of time having very enjoyable conversations, but these will achieve nothing. You'll have no results to show how it's working for you and no justification for the time and budget spent on it.

There is a wide range of objectives social media call help you with and I've listed an example of these below. Obviously, this list may not be right for your business and you won't know which objectives are right until you've analyzed the business plan and/or marketing strategy, but it gives you a good idea of the types of things you can achieve by using social media.

What tools do marketers use based on their weekly/hourly investment in Social Media?

- Building awareness
- Establishing thought leadership
- Launching new products or services
- Increasing reach (either geographically by sector)
- Generating leads
- Increasing sales
- Research and insight (understanding how to improve your product or service)
- Saving costs (e.g., reducing recruitment costs)
- Building your community
- Creating word-of-mouth activity
- Improving public relations activity
- ·Driving traffic to a website or blog
- Improving SFO
- Improving customer/client relations
- Providing customer/client service

•· Competitive analysis

Finding your Target Audience

Once you’ve profiled the people you want to connect with, you need to find them. This is an ongoing process and takes a little time to begin with. So, set some time aside to research where these people are.

There are a bunch of tools you can use to help you find them on the main social networks.

How to Find People on Twitter?

- **Scarch.twttrcr.com** is a favorite. It has a wide criteria range, including location (handy for local businesses). Also use this tool to find the key influencers in your industry and browse their follower/following lists. You could find some great people to connect with there.
- **Twitterrel** lets you find people talking about related topics
- **Twellow** is the Twitter equivalent of the Yellow Pages. A directory sorted by occupation. Handy.
- **Just Tweet** is a directory sorted by interest
- **WeFollow** is a directory that organizes people by hashtags.

Also pay attention to hashtags being used for events, you could find some great people there.

There are a few search tools for Twitter and some of these double up on features, so have a play around and see which suit your needs.

Let’s now look at the same information with your brand’s Twitter posts:

Date	**Twitter Followers**	**Twitter Posts**
May 1	100	One tweet to download white paper
May 2	101	Two tweets about latest product release
May 3	106	No tweets
May 4	106	Tweet asking customers for product feedback
May 5	100	Thank-you tweet for feedback

How to Find People on LinkedIn?

There aren’t so many tools to find people on LinkedIn as there are on Twitter, but there are a few options to search for the right people to connect with.

- Search for the names of those people you’ve already identified by name using LinkedIn’s search box. Also make the most of the advanced search feature.
- You can also use this search box to search for keywords that will be included in profiles. Make the most of using OR or AND in these searches to include a few keywords (OR allows you to look for any one of those terms in the profile, AND allows you to look for a number of words).

• You can also search for people using their email addresses. Join groups that fit with your interests or industry. Once you've been accepted as a member, browse the member lists and find people with shared interests

• Use the Questions and Answers function to start a conversation around your key subject area. You'll find those people interested will respond to you, after which you can connect with them.

• You can't simply choose to connect with people on LinkedIn as you can with Twitter. They need to give their approval (which I'm a fan of) .. so if they're connected to you through someone you're connected to, request to be introduced to them.

How to Find People on Facebook?

Again, it's not as easy to find people as it is on Twitter, but try these tips:

• Use the find people tool by popping your email address in. It finds all those people in your Address Book that are using Facebook.

• When using the search function, filter your results to drill down to the people you're looking for.

• Use the search for workmates function to find people affiliated with companies.

• Keep an eye on the suggestions that pop up on your news stream.

SOCIAL MEDIA CAN MAKE A BIG DIFFERENCE FOR EMAIL MARKETING

Still by far the most effective Digital Marketing tool, email marketing is an extremely cost effective way to reach current and prospective customers. It doesn't have to be complicated. Once you've got a basic system set-up, you can quickly send out newsletters, special offers and other updates to your mailing list.

• Far cheaper and more targeted than paper-based mailings.

• Send tailored emails to customers, based on their interests.

• Respond quickly to market conditions, technical issues or competitor promotions.

• Track precisely who has read your emails and what they have clicked on.

• Send out individual product updates or general newsletters.

• See exactly which links customers have clicked on and then follow up.

Brand Responses

How can people respond to Like Follow
your brand? Subscribe Unlike Unfollow
Unsubscribe Wall comment Mention

Discovery

Where do people go to find Twitter Feed
your content Inbox l-Facebook Twitter Search
News Feed Search Engines

Network Responses

Are there any delivery challenges? Bounces N/A N/A

Measure Your Success

Gauging the effectiveness of your SMM campaign isn't necessarily all exact science, but there are ways to know whether or not you're reaching people, or reaching out to the fight people. You can use analytics tools such as Google Analytics, which is tree and Omniture to measure how many visitors you're getting to your social media sites, how much time and how many pages they're viewing while they're on your page(s), and whether those guests are following through with a visit to your business website. Many of the social networking and SMM websites you join offer their own tools for measuring.

Simple SMM Do's and Don'ts

Do's

- Be open, honest and unselfish in your use of social media and networking applications.
- Address issues that are meaningful to your target audience. Put them first.
- Provide fresh insight and original content.
- Listen to your contacts and respond in a way that is meaningful and useful to them.
- Provide ways for people to contact you for additional support.
- Provide links to other useful resources. Remember, social media is about what you can do for others.

Don'ts

- Wait for an invitation: Reach out to your audience.
- Sneak in a sales pitch. This is a turn off to people looking for information and support.
- Talk too much about yourself or your company. Keep the focus on what's interesting to your audience.
- Forget to monitor your feedback and respond swiftly.
- 'Infrastructure that's equipped to handle traffic' spikes.

Electronic Money Transfer:

There are four essential security requirements for secure electronic payment which are described below:

IMPS

IMMEDIATE PAYMENT SERVICE

1. Authentication: A way to verify the buyer's identity before payments are made. Authentication is another issue in a Internet banking system. Transactions on the Internet or any other telecommunication network must be secure to achieve a high level of public confidence. In cyberspace, as in the physical world, customers, banks and merchants need assurances that they will receive the service as ordered or the merchandise as requested, and that they know the identity of the person they are dealing with.

Banks typically use symmetric (private key) encryption technology to secure messages and asymmetric (public/private key) cryptography to authenticate parties. Asymmetric cryptography employs two keys — a public key and a private key. These two keys are mathematically tied but one key cannot be deduced from the other. For example to authenticate that a message came from the sender, the sender encrypts the message using their private key.

Only the sender knows the private key. But, once sent, the message can be read only using the sender's public key. Since the message can only be read using the sender's public key, the receiver knows the message came from the expected sender.

Internet banking systems should employ a level of encryption that is appropriate to the

level or risk present in the systems. It is established that stronger levels of encryption may slow or degrade performance and, accordingly, management must balance security needs with performance and cost issues. Thus, a national bank should conduct a risk assessment in deciding upon it appropriate level of encryption. It does not mandate a particular strength or type of encryption. Rather, it expects management to evaluate security risks, review the cost and benefit of different encryption systems, and decide on an appropriate level of encryption as a business decision. Management should be able to explain the supporting analysis for their decision.

A common asymmetric cryptography system is RSA, which uses key lengths up to bits. By using the two forms of cryptography together, symmetric to protect the message and asymmetric to authenticate the parties involved, banks can secure the message and have a high level of confidence in the identity of the parties involved.

Biometric devices are an advanced form of authentication. These devices may take the form of a retina scan, finger or thumb print scan, facial scan, or voice print scan. Use of biometrics is not yet considered mainstream, but may be used by some banks for authentication.

2. Trust: Trust is another issue in Internet banking systems. As noted in the previous discussion, public and private key cryptographic systems can be used to secure information and authenticate parties in transactions in cyberspace. A trusted third party is a necessary part of the process. That third party is the certificate authority.

A certificate authority is a trusted third party that verifies identities in cyberspace. Some people think of the certificate authority functioning like an online notary. The basic concept is that a bank, or other third party, uses its good name to validate parties in transactions. This is similar to the historic role banks have played with letters of credit, where neither the buyer nor seller knew each other but both parties were known to the bank. Thus, the bank uses its good name to facilitate the transaction, for a fee. Banks also may need a way to validate themselves in cyberspace, as theft of identity has taken place. A proper mix of preventive, detective, and corrective controls can help protect national banks from these pitfalls. Digital certificates may play an important role in authenticating parties and thus establishing trust in

Internet banking systems. Ensuring that information will not be accidentally or maliciously altered or destroyed, usually during transmission.

3. Privacy: Privacy is a consumer issue of increasing importance. National banks that recognize and respond to privacy issues in a proactive way make this a positive attribute for the bank and a benefit for its customers. Public concerns over the proper versus improper accumulation and use of personal information are likely to increase with the continued growth of electronic commerce and the internet. Providers who are sensitive to these concerns have an advantage over those who do not.

4. Non-repudiation: Non-repudiation is the undeniable proof of participation by both the sender and receiver in a transaction. It is the reason public key encryption was developed, i.e., to authenticate electronic messages and prevent denial or repudiation by the sender or receiver. Although technology has provided an answer to non-repudiation, state laws are not uniform in the treatment of electronic authentication and digital signatures. The application of state laws to these activities is a new and emerging area of the law.

5. Availability: Availability is another component in maintaining a high level of public confidence in a network environment. All or the previous components are of little value if the network is not available and convenient to customers. Users of a network expect access to systems 24 hours per day, seven days a week. Among the considerations associated with system availability are capacity, performance monitoring, redundance, and business resumption.

National banks and their vendors who provide Internet banking products and services need to make certain they have the capacity in terms of hardware and software to consistently deliver a high level of service.

In addition, performance monitoring techniques will provide management with information such as the volume of traffic, the duration of transactions, and the amount of time customers must wait for service. Monitoring capacity, downtime, and performance on a regular basis will help management assure a high level of availability for their Internet banking system.

It is also important to evaluate network vulnerabilities to prevent outages due to component failures. An entire network can become inoperable when a single hardware component or software module malfunctions. Often, national banks and their vendors employ redundant hardware in critical areas or have the ability to switch to alternate processing locations. The latter is often referred to as contingency planning.

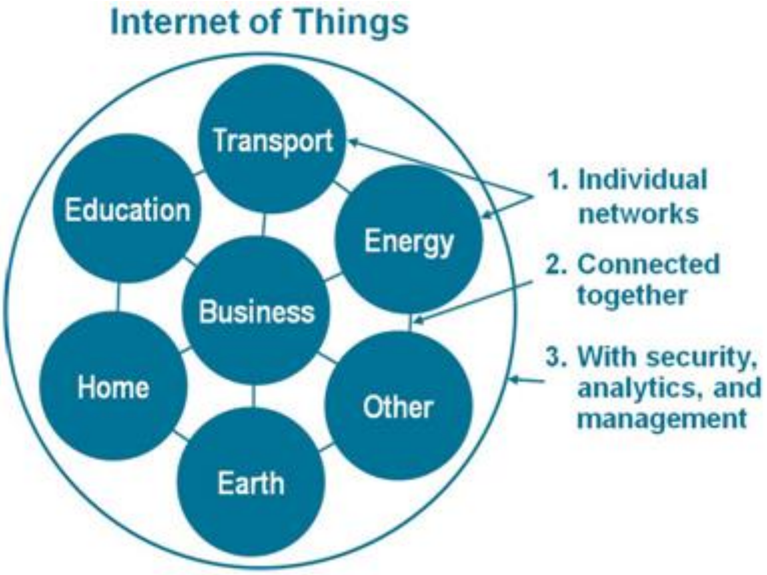
Mobile applications and Internet of Things (IOT)

The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data.

These devices collect useful data and Information with the help of various existing technologies and then autonomously flow the data between other devices. The figure is shown below depicting IOT.

The concept was introduced in 1999 to work together with physical and virtual world. How IOT works

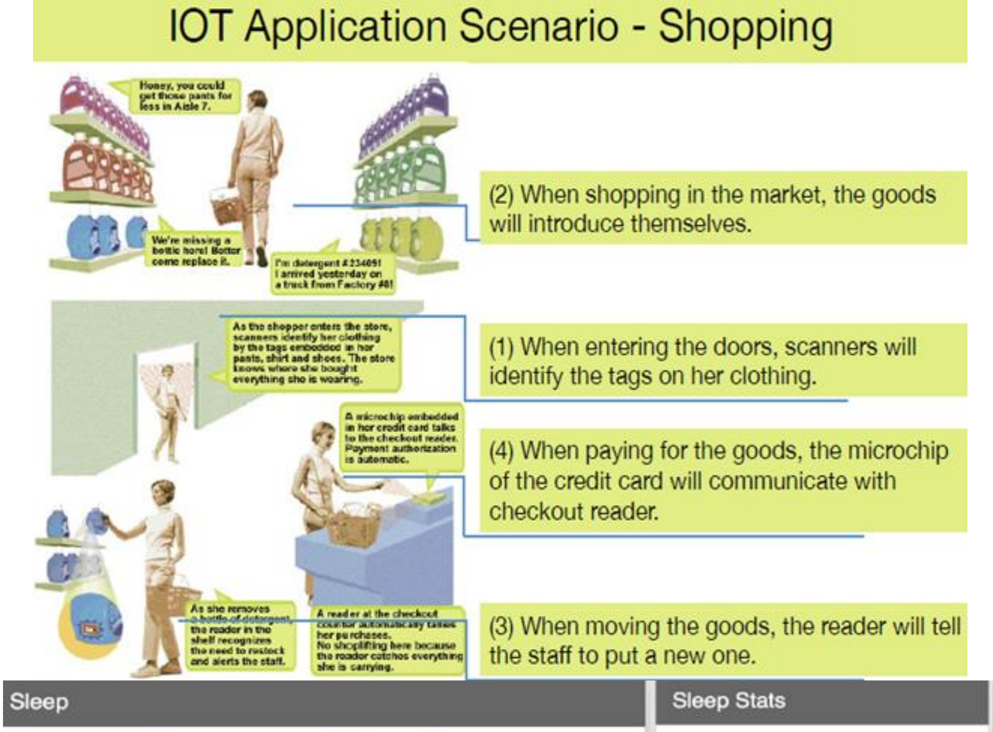
1. Actuation
2. Sensing
3. Identification
4. Addressability
5. Localization
6. User Interfaces



All networks are connected with security analytics and management and working together to provide better results in various fields.

Various Applications of IOT are mentioned below:

1. Building and Home Automation
2. Manufacturing
3. Medical and Health Care System



IOT Application Scenario - Shopping

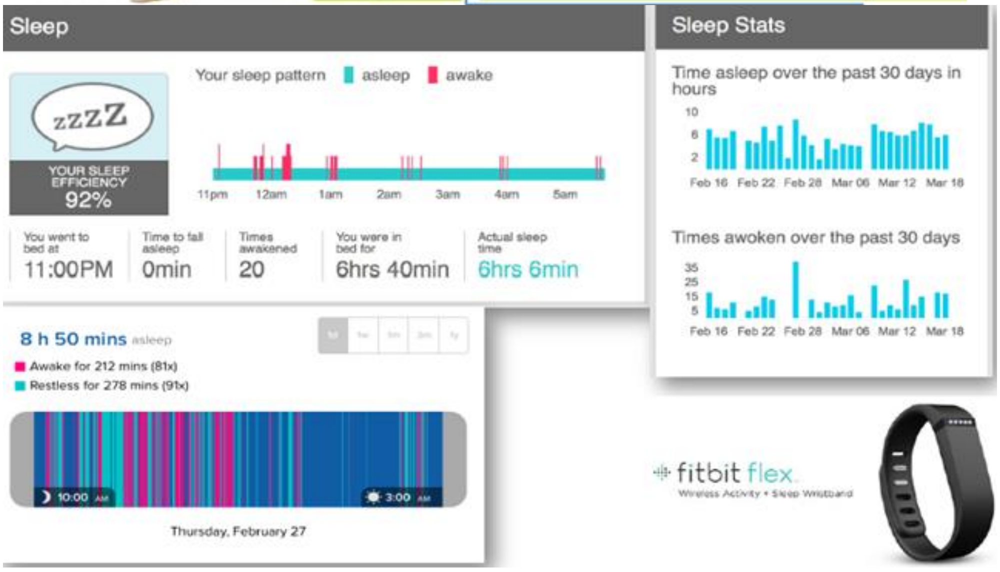
(2) When shopping in the market, the goods will introduce themselves.

(1) When entering the doors, scanners will identify the tags on her clothing.

(4) When paying for the goods, the microchip of the credit card will communicate with checkout reader.

(3) When moving the goods, the reader will tell the staff to put a new one.

Honey, you could get those pants for less in Aisle 7.
We're missing a bottle here! Better come replace it.
I'm detergent #23409! I arrived yesterday on a truck from Factory #8!
As the shopper enters the store, scanners identify her clothing by the tags embedded in her pants, shirt and shoes. The store knows where she bought everything she is wearing.
A microchip embedded in her credit card talks to the checkout reader. Payment authorization is automatic.
As she removes a bottle of detergent, the reader in the shelf recognizes the need to restock and alerts the staff.
A reader at the checkout counter automatically tallies her purchases. No shoplifting here because the reader catches everything she is carrying.



Sleep

Your sleep pattern 🟦 asleep 🟥 awake

zzzZ

YOUR SLEEP EFFICIENCY 92%

You went to bed at 11:00PM

Time to fall asleep 0min

Times awakened 20

You were in bed for 6hrs 40min

Actual sleep time 6hrs 6min

8 h 50 mins asleep

🟥 Awake for 212 mins (81x)

🟦 Restless for 278 mins (91x)

Thursday, February 27

Sleep Stats

Time asleep over the past 30 days in hours

Times awoken over the past 30 days

fitbit flex

Wireless Activity + Sleep Wristband

4. Media
5. Environmental Study and Monitoring
6. Manufacturing Management

7. Energy Management

8. Transportation

9. Better Quality of life

3.5 DOMAIN NAME

A domain name is a way to identify and locate computers connected to the Internet. No two organizations can have the same domain name.

A domain name always contains two or more components, separated by periods, called "dots." Some examples or domain names are: Godaddy, Internic.net, netsol.com, nasa.gov, delhi.edu, du.ac.in

Once a domain name has been established, "sub-domains" can be created within the domain. For example, the domain name for a large company could be "yahoo.com" and within this domain, sub-domains can be created for each of the company's regional offices.

hostname .subdomain.second- level domain.top-level domain

For example, india.yahoo.com a single host computer named a, Indian office of the Yahoo Company. Not all domain names will have a host name and sub-domain. In addition, more than one sub-domain can be assigned.

The top-level portion of a domain name describes the type of organization holding that name. The major categories for top-level domains are:

- COM – Commercial entities
- EDU – Four year colleges and universities
- NET – Organizations directly involved in Internet operations, such as network providers and network information centers
- ORG – Miscellaneous organizations that do not fit any other category, such as nonprofit group
- GOV – Government entities
- MIL – United States military
- COUNTRY CODES – a two letter abbreviation for a particular country. For example, "IN" for India or "UK" for United Kingdom.

Each domain name corresponds to numeric **IP** (Internet Protocol) addresses. An IP address takes the form of 4 numbers, each one between 0 and 255, separated by periods. The internet uses the numeric IP address to send data. For instance, you may be connecting to a World Wide Web server with the domain name "rs.internic.net", but as far as the network is concerned, you are connecting to the Web server with the IP address associated with that domain name.

The Domain Name System (DNS) completes the task of matching domain names to IP (Internet Protocol) addresses. Domain names and their corresponding IP addresses must be unique. If more than one organization on the internet had the same domain name, confusion would occur when the network tried to identify and communicate with the computers within those organizations.

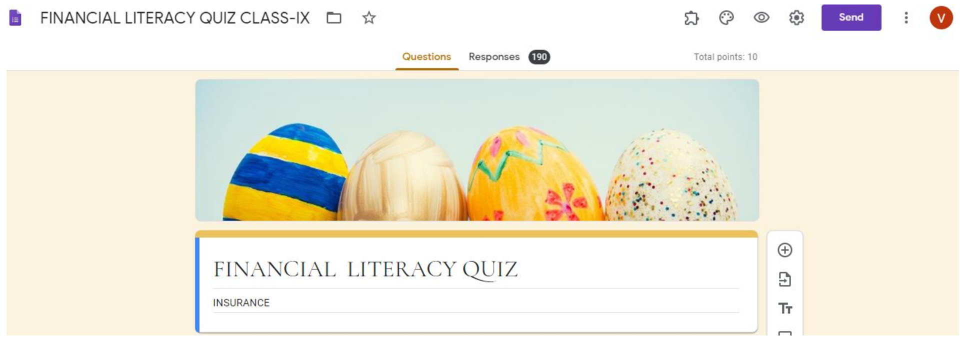
DNS is a collection of databases that contain information about domain names and their corresponding IP address.

Domain name servers: Domain name servers are computers that translate domain names to IP addresses. This system allows Internet users to deal with the more intuitive domain names, rather than having to remember a series of numbers.

Example:

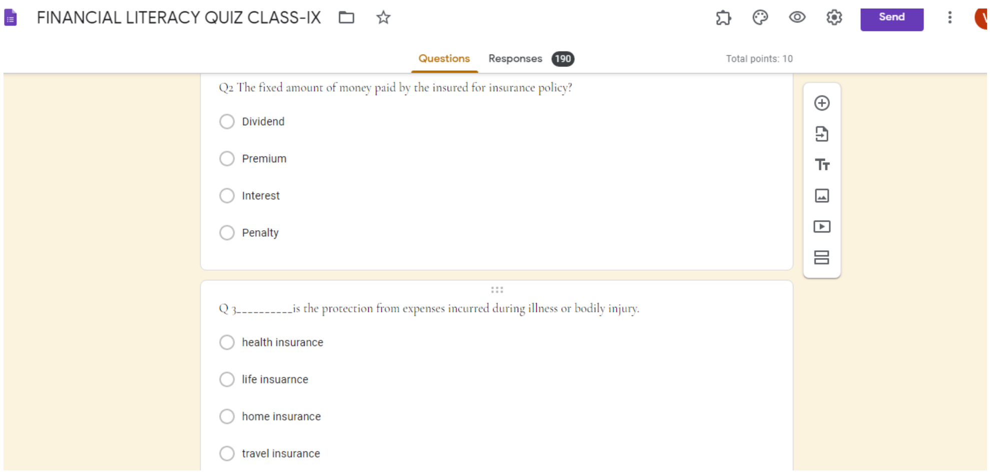
192.168.162.9

E Forms



FINANCIAL LITERACY QUIZ

INSURANCE



Q2 The fixed amount of money paid by the insured for insurance policy?

○ Dividend

○ Premium

○ Interest

○ Penalty

Q 3__________is the protection from expenses incurred during illness or bodily injury.

○ health insurance

○ life insuarnce

○ home insurance

○ travel insurance

EMoney

EMoney may be refer to as systems that enable bank customers to access accounts and general information on bank products and services through a personal computer (PC), Mibile or other Intelligent device.

Internet banking products and services can include wholesale products for corporate customers as well as retail and fiduciary products for consumers. Ultimately, the products and services obtained through Internet banking may be minor products and services offered through other bank delivery channels. Some examples of wholesale products and services include:

- Cash management.
- Wire transfer.
- Automated clearinghouse (ACH) transactions.
- Bill presentment and payment.

Examples of retail and fiduciary products and services include:

- Balance inquiry.
- Funds transfer.
- Downloading transaction information.
- Bill presentment and payment.
- Loan applications.
- Investment activity.
- Other value-added service.

In the past, the computer systems that made the information systems operate were rarely noticed by customers Today, websites, electronic mail and electronic bill presentment and payment systems are an important way for banks to reach their customers.

National banks have experimented with various forms of online banking for many years. Some of the early experimented involved closed systems where the customers accessed banks through a dial-in or cable TV connection. These systems limited a Bank potential customer base because they required out or area customers to either incur long-distance charges on their phone bills or subscribe to a particular cable TV service to access the bank. With the widespread growth or the Internet, customer can use this technology anywhere in the world to access a bank’s network. The Internet as an enabling technology has made banking products and services available to more customers and eliminated geographic and proprietary systems barriers. With an expanded market, banks also may have opportunities to expand or change their product and service offerings. Inter-bank Transfer is a special service that allows you to transfer funds electronically to accounts in other banks in India through:

NEFT – The acronym “NEFT” stands for National Electronic Funds Transfer. Funds are transferred to the credit account with the other participating Bank using RBI’s NEFT service.

RBI acts as the service provider and transfers the credit to the other bank’s account.

RTGS – The acronym “RTGS” stands for Real Time Gross Settlement. The RTGS system facilitates transfer of funds front accounts in one bank to another on a “real time” and on "gross settlement" basis. The RTGS system is the fastest possible inter-bank money transfer facility available through secure banking channels in India.

Minimum /Maximum amount for RTGS/NEFT transactions under Retail Internet Banking are following:

Type	**Minimum**	**Maximum**
RTGS	` 1 Lakh	` 5 Lakh
NEFT	No Limit	` 5 Lakh

And the minimum/maximum amount for RTGS/NEFT transactions under Corporate Internet Banking are following:

Type	**Minimum**	**Maximum**
RTGS	` 1 Lakh	No Limit
NEFT	No Limit	No Limit

Under normal circumstances, the beneficiary bank's branch receives the funds in real time as soon as funds are transferred by the remitting bank. The funds will be sent to the RBI within three hours of the transaction. The actual time taken to credit the beneficiary depends on the time taken by the beneficiary bank to process the payment.

Growth in E Money

Numerous factors including competitive cost, customer service and demographic considerations are motivating banks to evaluate their technology and assess their electronic commerce and Internet banking strategies. Many researchers expect rapid growth in customers using online banking products and services. The challenge for national banks is to make sure the savings from Internet banking technology more than offset the costs and risks associated with conducting business in cyberspace.

Marketing strategies will vary as national banks seek to expand their markets and employ lower cost delivery channels. Examiners will need to understand the strategies used and technologies employed on a bank-by-bank basis to assess the risk. Evaluating a bank's data on the use of their websites may help examiners determine the bank's strategic objectives, how well the bank is meeting its Internet banking product plan and whether the business is expected to be profitable.

Some of the market factors that may drive a bank's strategy include the following:

- ***Competition:*** Studies show that competitive pressure is the chief driving force behind increasing use of Internet banking technology, ranking ahead of cost reduction and revenue enhancement, in second and third place respectively. Banks see Internet banking as a way to keep existing customers and attract new ones to the bank.
- ***Cost Efficiencies:*** National banks can deliver banking services on the Internet at transaction costs far lower than traditional brick-and-mortar branches. The actual costs to execute a transaction will vary depending on the delivery channel used. For example,

according to Booz, Allen and Hamilton, as of mid-1 999, the cost to deliver manual transactions at a branch was typically more than a dollar, ATM and call center transactions cost about 25 cents, and internet transactions cost about a penny.

These costs are expected to continue to decline.

• National banks have significant reasons to develop the technologies that will help them deliver banking products and services by the most cost-effective channels.

However, national banks should use care in making product decisions.

• Management should include in their decision-making the development and ongoing costs associated with a new product or service, including the technology, marketing, maintenance and customer support functions. This will help management exercise due diligence, make more informed decisions and measure the success or their business venture.

• ***Geographical Reach:*** Internet banking allows expanded customer contact through increased geographical reach and lower cost delivery channels. In fact, some banks are doing business exclusively via the Internet — they do not have traditional banking offices and only reach their customers online. Other financial institutions are using the Internet as an alternative delivery channel to reach existing customers and attract new customers.

• ***Branding:*** Relationships building is a strategic priority of many national banks. Internet banking technology and products can provide a means for national banks to develop and maintain all ongoing relationship with their customers by offering easy access to a broad array of products and services. By capitalizing on brand identification and by providing a broad array of financial services, banks hope to build customer loyalty, cross-sell and enhance repeat business.

• ***Customer Demographics:*** Internet banking allows national banks to offer a wide array of options to their banking customers. Some customers will rely on traditional branches to conduct their banking business. For many, this is the most comfortable way for them to transact their banking business. Those customers place a premium on person-to-person contact. Other customers are early adopters of new technologies that arrive in the marketplace. These customers were the first to obtain PCs and the first to employ them in conducting their banking business The demographics of banking customers will continue to change. The challenge to national banks is to understand their customer base and find the right mix of delivery channels to deliver products and services profitably to their various market segments.

Types of e money/Internet Banking

Understanding the various types of Internet banking products will help examiners assess the risks involved. Currently, the following three basic kinds of Internet banking are being employed in the marketplace:

(a) International: This is the basic level of Internet banking. Typically, the bank has marketing information about the bank’s products and services on a standalone server.

The risk is relatively low, as informational systems typically have no path between the server and the bank’s internal network. This level of Internet banking can be provided by the bank or outsourced. While the risk in a bank is relatively low, the server or website may be vulnerable to alteration. Appropriate controls, therefore, must be in place to prevent unauthorized alterations to the bank’s server or website.

(b) Communicative: This type of Internet banking system allows some interaction between the bank's systems and the customer, electronic mail, account inquiry, loan applications, or static file updates. Because these servers may have a path to the bank's internal networks, the risk is higher with this configuration than with informational systems. Appropriate controls need to be in place to prevent monitor and alert management of any unauthorized attempt to access the bank's internal networks and computer systems. Virus controls also become much more critical in this environment.

(c) *Transactional:* This level of Internet banking allows customers to execute transactions. Since a path typically exists between the server and the bank's or outsourcer's internal network, this is the highest risk architecture and must have the strongest controls. Customer transactions can include accessing accounts paying bills, transferring funds, etc.

Emoney/Banking Risks

Internet banking creates new risk control challenges for national banks. From a supervisory perspective, risk is the potential that events, expected or unexpected, may have an adverse impact on the bank's earnings or capital. There are nine defined categories of risk for bank supervision purposes. The risks are credit, interest rate, liquidity, price, foreign exchange, transaction, compliance, strategic and reputation. These categories are not mutually exclusive and all of these risks are associated with Internet banking.

Credit Risk: Credit risk is the risk to earnings or capital arising from an obligor's failure to meet the terms of any contract with the bank or otherwise to perform as agreed. Credit risk is found in all activities where success depends on counterparty, issuer, or borrower performance.

It arises any time bank funds are extended, committed. invested, or otherwise exposed through actual or implied contractual agreements, whether on- or off-the-bank's balance sheet. Internet banking provides the opportunity for banks to expand their geographic range Customers can reach a given institution front literally anywhere in the world. Verifying collateral and perfecting security agreements also can be challenging with out-of-area borrowers. Unless properly managed, Internet banking could lead to a concentration in out-of-area credits or credits within a single industry. Moreover, the question of which state's or country's laws control all Internet relationship is still developing.

Fig. 6.7: Payment Process

Effective management of a portfolio of loans obtained through the Internet requires that the board and management understand and control the bank's lending risk profile and credit culture. They must assure that effective policies, processes and practices are in place to control the risk associated with such loans.

Interest rate risk: Interest rate risk is the risk to earnings or capital arising from movements in interest rates. From an economic perspective, a bank focuses on the sensitivity of the value of its assets, liabilities and revenues to changes in interest rates. Interest rate risk arises from differences between the timing of rate changes and the timing of cash flows (reprising risk); from changing rate relationships among different yield curves affecting bank activities (basis risk); from changing rate relationships across the spectrum of maturities (yield curve risk); and from interest-related options embedded in bank products (options risk). Evaluation of interest rate risk must consider the impact of complex, illiquid hedging strategies or products, and also the potential impact that changes in interest rates will have on the income. In those situations where trading is separately managed, this refers to structural positions and not trading portfolios.

Internet banking can attract deposits, loans, and other relationships from a larger pool of possible customers than other forms of marketing. Greater access to customers who primarily seek the best rate or term reinforces the need for managers to maintain appropriate asset/ liability management systems, including the ability to react quickly to changing market conditions.

Liquidity Risk: Liquidity risk is the risk to earnings or capital arising from a bank's inability to meet its obligations when they come due, without incurring unacceptable losses. Liquidity risk includes the inability to manage unplanned changes in funding sources. Liquidity risk also arises from the failure to recognize or address chances in market conditions affecting the ability of the bank to liquidate assets quickly and with minimal loss in value. Internet banking can increase deposit volatility from customers who maintain accounts solely on the basis of rate or terms. Asset/liability and loan portfolio management systems should be appropriate for products offered through Internet banking. Increased monitoring of liquidity and changes in deposits and loans may be warranted depending on the volume and nature of Internet account activities.

Price Risk: Price risk is the risk to earnings or capital arising from changes in the value of traded portfolios of financial instruments. This risk arises from market making, dealing and position taking in interest rate, foreign exchange, equity and commodities markets. Banks may be exposed to price risk if they create or expand deposit brokering, loan sales, or securitization programs as a result of Internet banking activities. Appropriate management systems should be maintained to monitor, measure and manage price risk if assets are actively traded.

Foreign Exchange Risk: Foreign exchange risk is present when a loan or portfolio of loans is denominated in a foreign currency or is funded by borrowings in another currency.

In some cases, banks will enter into multi-currency credit commitments that permit borrowers to select the currency they prefer to use in each rollover period. Foreign exchange risk can be intensified by political, social or economic developments. The consequences can be unfavorable if one of the currencies involved becomes subject in stringent exchange controls or is subject to wide exchange-rate fluctuations. Banks may be exposed to foreign exchange risk if they accept deposits from non-US residents or create accounts denominated in currencies other than US dollars. Appropriate systems should be developed if banks engage in these activities.

Transaction Risk: Transaction risk is the current and prospective risk to earnings and capital arising from fraud, error, and the inability to deliver products or services maintain a competitive position, and manage information. Transaction risk is evident in each product and service offered and encompasses product development and delivery, transaction processing, systems development, computing systems, complexity of products and services, and the internal control environment.

A high level of transaction risk may exist with Internet banking products, particularly if those lines of business are not adequately planned, implemented and monitored. Banks that offer financial products and services through the Internet must be able to meet their customers' expectations. Banks must also ensure they have the right product mix and capacity to deliver accurate, timely and reliable services to develop a high level of confidence in their brand name.

Customers who do business over the Internet are likely to have little tolerance for errors or omissions from financial institutions that do not have sophisticated internal controls to manage their Internet banking business. Likewise, customers will expect continuous availability of the product and Web pages that are easy to navigate.

Software to support various Internet banking functions is provided to the customer from a variety of sources. Banks may support customers using customer-acquired or bank-supplied browsers or personal financial manager (PFM) software. Good communications between banks and their customers will help manage expectations on the compatibility of various PFM software products.

Attacks or intrusion attempts on banks' computer and network systems are a major concern.

Studies show that systems are more vulnerable to internal attacks than external, because internal system users have knowledge of the system and access. Banks should have sound preventive and detective controls to protect their Internet banking systems from exploitation both internally and externally.

Contingency and business resumption planning is necessary for banks to be sure that they can deliver products and services in the event of adverse circumstances. Internet banking products connected to a robust network may actually make this easier because back-up capabilities can be spread over a wide geographic area. For example, if the main server is inoperable, the network could automatically reroute traffic to a back-up server in a different geographical location. Security issues should be considered when the institution develops its contingency and business resumption plans. In such situations, security and internal controls at the back-up location should be as sophisticated as those at the primary processing site. High levels of system availability will be a key expectation of customers and will likely differentiate success levels among financial institutions on the Internet.

Electronic Payment Systems 187

National banks that offer bill presentment and payment will need a process to settle transactions between the bank, its customers and external parties. In addition to transaction risk, settlement failures could adversely affect reputation, liquidity and credit risk.

Compliance Risk: Compliance risk is the risk to earnings or capital arising from violations of, or non-conformance with, laws, rules, regulations, prescribed practices or ethical standards. Compliance risk also arises in situations where the laws or rules governing certain bank products or activities of the bank's clients may be ambiguous or untested. Compliance risk exposes the institution to fines, civil money penalties, payment of damages and the voiding of contracts.

Compliance risk can lead to a diminished reputation, reduced franchise value, limited business opportunities, reduced expansion potential and lack of contract enforceability. Most Internet banking customers will continue to use other bank delivery channels. Accordingly, national banks will need to make certain that their disclosures on Internet banking channels, including websites, remain synchronized with other delivery channels to ensure the delivery of a consistent and accurate message to customers.

Federal consumer protection laws and regulations, including CRA and Fair Lending, are applicable to electronic financial services operations including Internet banking. Moreover, it is important for national banks to be familiar with the regulations that permit electronic delivery of disclosures/notices versus those that require traditional hard copy notification. National banks should carefully review and monitor all requirements applicable to electronic products and services and ensure they comply with evolving statutory and regulatory requirements.

Advertising and record-keeping requirements also apply to banks' websites and to the products and services offered.

Regular monitoring of bank websites will help ensure compliance with applicable laws, rules and regulations.

Application of Bank Secrecy Act (USA) requirements to cyber banking products and services is critical. The anonymity of banking over the Internet poses a challenge in adhering to BSA standards.Also, the bank should set up a control system to identify unusual or suspicious activities and, when appropriate, file suspicious activity reports (SARs).

The BSA funds transfer rules also apply to funds transfers or transmittals performed over the Internet when transactions exceed $3,000 and do not meet one of the exceptions. The rules require banks to ensure that customers provide all the required information before accepting transfer instructions. The record keeping requirements imposed by the rules allow banks to retain written or electronic records of the information.

Strategic Risk

Strategic risk is the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation. The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities. The organization's internal characteristics must be evaluated against the impact of economic, technological, competitive, regulatory and other environmental changes. Management must understand the risks associated with Internet banking before they make a decision to develop a particular class of business. In some cases, banks may offer new products and services via the Internet. It is important that management understand the risks and ramifications of these decisions.

Sufficient levels of technology and MIS are necessary to support such a business venture. Because many banks will compete with financial institutions beyond their existing trade area, those engaging in Internet banking must have a strong link between the technology employed and the bank's strategic planning process.

Before introducing a Internet banking product, management should consider whether the product and technology are consistent with tangible business objectives in the bank's strategic plan. The planning and decision-making process should focus on how a specific business need is met by the internet banking product, rather than focusing on the product as an independent objective.

The bank's technology experts, along with its marketing and operational executives, should contribute to the decision-making and planning process. They should ensure that the plan is consistent with the overall business objectives of the bank and is within the bank's risk tolerance.

New technologies, especially the Internet, could bring about rapid changes in competitive forces. Accordingly, the strategic vision should determine the way the Internet banking product line is designed, implemented and monitored.

Reputation Risk

Reputation risk is the current and prospective impact on earnings and capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services or continue servicing existing relationships. This risk may expose the institution to litigation, financial loss, or a decline in its customer base. Reputation risk expose is present throughout the organization and includes the responsibility to exercise an abundance of caution in dealing with customers and the community.

A bank's reputation can suffer if it fails to deliver on marketing claims or to provide accurate, timely services. This can include failing to adequately meet customer credit needs, providing unreliable or inefficient delivery systems, untimely responses to customer inquiries or violations of customer privacy expectations.

Electronic Payment S

A bank's reputation can be damaged by Internet banking services that are poorly executed or otherwise alienate customers and the public. Well designed marketing, including disclosures, is one way to educate potential customers and help limit reputation risk. Customers must understand what they can reasonably expect from product or service, and what special risks and benefits they incur when using the system such marketing concepts need to be coordinated closely with adequate disclosure statements. A national bank should not market the bank's Internet banking system based on features or attributes that system does not have. The marketing program must present the product fairly and accurately. National banks should carefully consider how connections to third parties are presented on their websites. Hypertext links are often used to enable a customer to link to a third party.

Such links may reflect an endorsement of the third party's products or services in the eyes of the customer. It should be clear to the customer when they have left the bank's website so that there is no confusion about the provider of the specific products and services offered or the security and privacy standards that apply. Similarly, adequate disclosures must be made so that customers can distinguish between insured and non-insured products.

National banks need to be sure that their business continuity plans include the Internet banking business. Regular testing of the business continuity plan, including communications strategies with the press and public, will help the bank ensure it can respond effectively and promptly to any adverse customer or media reactions.

Risk Management

Financial institutions should have a technology risk management process to enable them to identify, measure, monitor and control their technology risk exposure. Risk management of new technologies has three essential elements:

- The planning process for the use of the technology.

- The implementation of the technology.
- The means to measure and monitor risk.

The *OCC's* objective is to determine whether bank is operating its Internet banking business in a safe and sound manner. The OCC expects banks to use a rigorous analytic process to identify, measure, monitor and control risk. Examiners will determine whether the level of risk is consistent with the bank's overall risk tolerance and is within the bank's ability to manage and control.

The risk planning process is the responsibility of the board and senior management. They need to possess the knowledge and skills to manage the bank's use of Internet banking technology and technology-related risks. The board should review, approve and monitor Internet banking technology-related projects that may have a significant impact on the bank's risk profile. They should determine whether the technology and products are in line with the bank's strategic goals and meet a need in their market. Senior management should have the skills to evaluate the technology employed and risks assumed.

190 E-Commerce

Periodic independent evaluations of the Internet banking technology and products by auditors or consultants can help the board and senior management fulfill their responsibilities.

Implementing the technology is the responsibility of management. Management should have the skills to effectively evaluate Internet banking technologies and products, select the right mix for the bank, and sec that they are installed appropriately. If the bank does not have the expertise to fulfill this responsibility internally, it should consider contract with a vendor who specializes in this type of business or engaging, in an alliance with another provider with complementary technologies or expertise.

Measuring and monitoring risk is the responsibility of management. Management should have the skills to effectively identify, measure, monitor and control risks associated with Internet banking. The board should receive regular reports on the technologies employed, the risks assumed and how those risks are managed. Monitoring system performance is a key success factor. As a part of the design process, a national bank should include effective quality assurance and audit processes in its Internet banking system. The bank should periodically review the systems to determine whether they are meeting the performance standards.

Internal Controls

Internal controls over Internet banking systems should be commensurate with all institution's level of risk. As in any other banking area, management has the ultimate responsibility for developing and implementing a sound system of internal controls over the bank's Internet banking technology and products.

Regular audits of the control systems will help ensure that the controls are appropriate and functioning properly. For example, the control objectives for an individual bank's Internet banking technology and products might focus on:

- Consistency of technology planning and strategic goals, including efficiency and economy of operations and compliance with corporate policies and legal requirements.
- Data availability, including business recovery planning.

- Data integrity, including providing for the safeguarding of assets, proper authorization of transactions and reliability of the process and output.
- Data confidentiality and privacy safeguards.
- Reliability of MIS.

Once control objectives are established, management has the responsibility to install the necessary internal controls to see that the objectives are met. Management also has the responsibility to evaluate the appropriateness of the controls on a cost-benefit basis. That analysis may take into account the effectiveness of each control in a process, the dollar volume flowing through the process and the cost of the controls.

Electronic Payment Systems 191

Examiners will need to understand the bank's operational environment to evaluate the proper mix of internal controls and their adequacy. According to the Information Systems Audit and Control Association (ISACA), the basic internal control components include:

- **Internal accounting controls:** Used to safeguard the assets and reliability of financial records. These would include transaction records and trial balances.
- **Operational controls:** Used to ensure that business objectives are being met. These would include operating plans and budgets to compare actual against planned performance.
- **Administrative controls:** Used to ensure operational efficiency and adherence to policies and procedures. These would include periodic internal and external audits. ISACA separates internal controls into three general categories. The three control categories

can be found in the basic internal controls discussed above.

- **Preventive controls:** Prevent something (often an error or illegal act) from happening. An example of this type of control is logical access control software that would allow only authorized persons to access a network using a combination of a user ID and password.
- **Detective controls:** Identify an action that has occurred. An example would be intrusion detection software that triggers an alert or alarm.
- **Corrective controls:** Correct a situation once it has been detected. An example would be software back-ups that could be used to recover a corrupted file or database. Banks or service providers offering transaction-based Internet banking products need to have a high level of controls to help manage the bank's transaction risk. Examples of these controls could include:
- Monitoring transaction activity to look for anomalies in transaction types, transaction volumes, transaction values and time-of-day presentment.
- Monitoring log-on violations or attempts to identify patterns of suspect activity including unusual requests, unusual timing or unusual formats.
- Using trap and trace techniques to identify the source of the request and match these against known customers. Regular reporting and review of unusual transactions will help identify:
- Intrusions by unauthorized parties.
- Customer input errors.
- Opportunities for customer education.

Regulations of PPI (Pre-Payment Instruments) by RBI,

Regulations of Pre-payment Instruments were updated on 13th April, 2020 by the Reserve Bank of India. The following topics covered in the PPI:

1. What Powers has RBI?
2. What is PPI?
3. Who are issuers of PPI?
4. Who is the holder of PPI?
5. What are types of PPI?
6. What are the types of semi-closed PPI?

Unit IV

ELECTRONIC RECORDS

- Authentication of Electronic Records;
- Legal Recognition of Electronic Records;
- Legal Recognition of Digital Signatures;
- Applications and usage of electronic records and Digital Signatures in Government and its Agencies;
- Retention of Electronic Records,
- Intermediaries and their liabilities;
- Attribution, Acknowledgement and Dispatch of Electronic Records;
- Secure Electronic Records and Digital Signatures.
- Summary
- Exercise

4.1 AUTHENTICATION OF ELECTRONIC RECORDS

The Information Technology Act, 2000 (ITA 2000) gives the provisions of authentication of electronic records. This chapter was amended by the Information Technology (Amendment) Act, 2008 (ITAA 2008). The ITAA 2008 substituted the word “digital signature” by “electronic signature”.

The section provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature. The digital signature is created in two distinct steps. First the electronic record is converted into a message digest by using a mathematical function known as “hash function” which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature. Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message. In ITA 2000, this section is given as follows:

[Section 3] Authentication of electronic records.

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his Digital Signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation - For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible –

   (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

   (b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

Section 3A provides authentication of records by using any electronic signature or electronic authentication technique, which is considered reliable and mentioned in the second schedule. However, no such technique is mentioned in the second schedule. As per ITAA 2008 section 3A:

(1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which –

   (a) is considered reliable ; and

   (b) may be specified in the Second Schedule

(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if –

   (a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

   (b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

   (c) any alteration to the electronic signature made after affixing such signature is detectable

   (d) any alteration to the information made after its authentication by electronic signature is detectable; and

   (e) it fulfills such other conditions which may be prescribed.

(3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated

(4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule;

   Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable

(5) Every notification issued under sub-section (4) shall be laid before each House of Parliament

From the above legal provisions, it is clear that any electronic signature or electronic authentication technique can be considered reliable if the authentication or signature creation data are within the context in which they are used. They should also be linked to the signatory or the authenticator only. If any alteration has been made to the electronic signature after affixing, it should be detectable. Moreover, electronic signatory or authenticator may be required to fulfill other conditions that may be prescribed the Central Government.

The Central Government is empowered to prescribe the procedure by notification in the Official Gazette for ascertaining weather the electronic signature is of the person who has affixed it. The Central Government has the right to add or omit any electronic signature or electronic authentication technique from the Second Schedule. However, such signature or authentication technique shall not be included in the Second Schedule if they are not reliable.

4.2 LEGAL RECOGNITION OF ELECTRONIC RECORDS

ITA 2000 gives the provisions of electronic governance. This chapter has adopted the 'functional-equivalent' approach. This approach is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques. The 'functional-equivalent' approach extended notions such as "writing", "signature" and "original" of traditional paper-based requirements to electronic form.

When adopting 'functional-equivalent' approach in the UNCITARL Model Law, attention was given to the existing hierarchy of form requirements, which provides distinct level of reliability, traceability and inalterability with respect to paper-based documents. This approach singles out the basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by electronic documents, enable such e-documents to enjoy the same level of legal recognition as corresponding paper documents performing the same function enjoy. For example, if a contract is signed and sent as an electronic document, the chances of its reliability would be, in general situations, lesser than that of a paper-based document due to certain doubts as to its authenticity and chances of alteration of the contents. However, if the same electronic document is sent after being digitally signed by using a digital signature certificate issued by a trustworthy digital signature certificate provider, then, since it would be able to perform the same functions of reliability, traceability and inalterability as a paper-based document, it would receive legal sanction. What is noticeable is that a document in electronic form can, with suitable technical guards, perform the functions of writing much better than a paper-based document.

For the purpose of this Unit, definition of 'electronic form', as provided under section 2(r) of the ITA 2000, is very material. It means, with reference to information, any information generated, sent, received, or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device.

ITA 2000 specifies the procedures to be followed for sending and receiving of electronic records and the time and the place of the despatch and receipt. This Unit contains sections 4 to 10. Certain amendments were made to this Unit by the ITAA 2008.

Section 4 of ITA 2000 provides for “legal recognition of electronic records”. It provides that where any law requires that any information or matter should be in the typewritten or printed form then such requirement shall be deemed to be satisfied if it is in an electronic form. This section is as follows:

[Section 4] Legal recognition of electronic records.

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, such requirements shall be in writing or in the typewriting or printed form, then, such requirements shall be in deemed to have been satisfied if such information or matter is -

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference

The word ‘accessible’, as per the UNCITRAL guide, is meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained. The word ‘usable’ is not intended to cover only human use but also computer processing. ‘Subsequent reference’ seems to imply merely the need for future reference. The carefully worded section does not seem to lay down any stringent standards as to the reliability or durability of the electronic record. Rather, it merely requires that such information if made available at a certain point of time in electronic form should be available for usage at some future time as well. The purpose is to basically provide a legal sanctity to production of any information in electronic form. Whether such information provided is correct, or authentic, or unaltered, or reliable is not within the purview of this section. If the law provides something to be in writing, then, subject to certain conditions, the legal requirement of writing would be fulfilled if such information is in electronic form.

It is clear that this section gives validity and recognizes the use of electronic records in place of the ordinary paper based records. This section effectively allows replacement of physical letters and transactions by the use of email and electronic means of communication. This is the most important section of the ITA 2000 and truly empowers the country to move towards electronic communication. The section states that in spite of anything contained in any other Act, electronic means may be used in place of the conventional written or paper based system. So as per the provisions of this section, electronic invoices, electronic receipts, SMS tickets for railways, email tickets are all valid records. An email sent as a Right to Information (RTI) application is also considered valid provided it fulfills other provisions of the Act.

4.3 LEGAL RECOGNITION OF DIGITAL SIGNATURES

Section 5 of ITA 2000 proceeds on the ‘functional-equivalent’ approach. It is based on the recognition of the functions of a signature in a paper-based environment. The following functions of a signature are considered in the UNCITRAL guide:

(a) identifying a person;

(b) providing certainty as to the personal involvement of that person in the act of signing;

(c) associating such person with the content of the document.

Broadly, these being the functions of a signature, the purpose of section 5 is to merely introduce and give legal sanctity and acceptance to the use of digital signatures. It is not necessary as to what is the mode of signature; it may be paper-based or electronic. However, so long as the functions of the signature are being performed, such signature will receive legal recognition.

Section 5 of the ITA 2000 states that –

[Section 5] Legal recognition of digital signature.

Where any law provides that any information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation - For the purposes of this section, "signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "signature" shall be construed accordingly.

The explanation to the section further clarifies the ambit of the word ‘signature’ as to mean, ‘with its grammatical variations and cognate expressions, with reference to a person, affixed of his hand written signature or any mark on any document’.

Section 5 of ITA 2000, like section 4, has a limited field of operation. It is not the purpose of section 5 to ascertain whether the digital signature affixed is as per the rules prescribed, or whether the functions of a signature have been fulfilled. The purpose is merely to provide legal recognition to a digital signature on par with hand-written signature wherever the law requires the affixation of such signature.

4.4 USE OF ELECTRONIC RECORDS AND DIGITAL SIGNATURES IN GOVERNMENT AND ITS AGENCIES

Section 6 of ITA 2000 lays down the foundation of electronic governance. The section meant to facilitate electronic filing of documents with the Government agencies and to promote efficient delivery of Government services by means of reliable electronic records. It provides for use of electronic records and digital signatures in government functioning. This section states that –

[Section 6] Use of electronic records and digital signatures in Government and its agencies.

(1) Where any law provides for—

(a) the filing of any form. application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;

(b) the issue or grant of any licence, permit, sanction or approval by whatever name called in a particular manner;

(c) the receipt or payment of money in a particular manner,

then, not with standing anything contained in any other law for the time being in force, such requirement shall be deemed to have been satisfied if such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe—

(a) the manner and format in which such electronic records shall be filed, created or issued;

(b) the manner or method of payment of any fee or charges for filing, creation or issue any electronic record under clause (a).

It is clear from section 6 that if any particular law requires filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner, or the issuance or grant of any licence, permit, sanction or approval by whatever name called in a particular manner, or the receipt or payment of money in a particular manner, then, under sub-section (1) of the section 6, such requirement would be deemed to have been satisfied if such filing, issue, grant, receipt or payment, is effected by means of an electronic form. Such electronic form may be prescribed by the appropriate government. The appropriate government, under sub-section (2), has been given the power to make rules to prescribe the manner and format in which such electronic records shall be filed, created or issued, as also the manner or method of payment of any fee or charges for filing, creation or issuance of any electronic record.

Therefore, an application for a document say, a land record, if made in the prescribed electronic form to the revenue and land records department, it would be legally valid under section 6. Or, a grant of certificate of registration as a dealer by the government under a sales tax legislation in an electronic form is now legally recognizable.

Section 6A was inserted by the ITAA 2008. As per section 6A –

(1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify, by notification in the Official Gazette.

Explanation - For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor form or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

(2) The appropriate Government may also authorize any service provider authorized under sub-section (1) to collect, retain and appropriate service charges, as may be prescribed by the appropriate Government for the purpose of providing such services, from the person availing such service.

(3) Subject to the provisions of sub-section (2), the appropriate Government may authorize he service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under

the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.

(4) The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the service providers under this section:

(5) Provided that the appropriate Government may specify different scale of service charges for different types of services.

It is clear that Section 6A of the ITAA 2008 contains provisions for efficient delivery of services to the public through electronic means. It talks about the service provider as the appropriate government may authorize any service provider and vary charges as it thinks fit. Every service provider needs due authorization to:

(a) function as a service provider (for a time period, as decided by the appropriate Government),

(b) provide prescribed services only, and

(c) collect and retain such appropriate e-service charges (or scale of service charges thereof) as prescribed.

4.5 RETENTION OF ELECTRONIC RECORDS

Various statutes provide for storage of information (for example, for tax purposes or auditing/accounting, etc.). Such information is generally stored on paper-based mode. However, with increase in computers for processing and storage of information, it became imperative to provide legal sanction to storage of information in electronic form. Modern trade works through information technology and requires it to retain all the information, though generated, sent or received in electronic form. If the information has to be retained in paper-based mode, then it would be a step back.

Section 7 of the ITA 2000 permits retention of information in electronic form and gives legal recognition to retention of electronic records. It provides that the documents, records or information which is to be retained for any specified period shall be deemed to have been retained if the same is retained in the electronic form provided the following conditions are satisfied:

(i) The information therein remains accessible so as to be usable subsequently.

(ii) The electronic record is retained in its original format or in a format which accurately represents the information contained.

(iii)The details which will facilitate the identification of the origin, destination, dates and time of despatch or receipt of such electronic record are available therein.

The section deems the fulfilment of the legal requirement of paper-based retention of information if the same is done in electronic form. However, this section does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received. Moreover, this section does not apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records. Further, the section provides no time period of retention of records in electronic form. Records pertaining to any subject matter should be retained in electronic form for that duration as mandated under that specific legal framework for the time being in force.

The section 7 of ITA is as follows:

[Section 7] Retention of electronic records.

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if—

(a) the information contained therein remains accessible so as to be usable for a subsequent reference;

(b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

(2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

This section should be read with section 67C of the ITAA 2008. Section 67 of the ITAA 2008 provides that the intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. In case of non-compliance of aforesaid provision by an intermediary intentionally or knowingly, the said intermediary be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

ITAA 2008 has inserted the section 7A. As per this section –

[Section 7A] Audit of documents in electronic form.

Where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

It should be noted that Section 7A of the ITAA 2008 is another step towards creating ‘functional equivalence’. It articulates that where in any law for the time being in force, there is a provision for audit of documents, records or information, that provision shall also be applicable for audit of documents, records or information processed and maintained in electronic form.

4.6 INTERMEDIARIES AND THEIR LIABILITIES

Governments all over world increasing press intermediaries to block their users undesirable internet contents, privacy violation etc.

4.7 ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS

IT Act deals with attribution, receipt and despatch of electronic records. Section 11 lays down how an electronic record is to be attributed to the person who originated it. ‘Attribution’ means ‘to consider it to be written or made by someone’. Section 12 provides for the manner in which acknowledgement of receipt of an electronic record by various modes shall be made. Whereas, Section 13 of the act provides for the manner in which the time and place of despatch and receipt of electronic record sent by the originator shall be identified. Generally, an electronic record is deemed to be despatched at the place where the originator has his place of business and received where the addressee has his place of business.

Section 11 is as follows:

[Section 11] Attribution of electronic records.

An electronic record shall be attributed to the originator

(a) if it was sent by the originator himself;

(b) by a person who had the authority to act on behalf of the originator in respect of that electronic record; or

(c) by an information system programmed by or on behalf of the originator to operate automatically.

As per ITAA 2008, Section 12 is given as under:

[Section 12] Acknowledgement of receipt (Modified by ITAA 2008).

(1) Where the originator has not stipulated that the acknowledgment of receipt of electronic record be given in a particular form or by a particular method, an acknowledgment may be given by -

  (a) any communication by the addressee, automated or otherwise; or

  (b) any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(2) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

(3) Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit, he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

As per ITA 2000, section 13 is as follows:

[Section 13] Time and place of despatch and receipt of electronic record.

(1) Save as otherwise agreed to between the originator and the addressee, the despatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

(2) Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely -

(a) if the addressee has designated a computer resource for the purpose of receiving electronic records -

(i) receipt occurs at the time when the electronic record enters the designated computer resource; or

(ii) if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee;

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

(3) Save as otherwise agreed between the originator and the addressee, an electronic record is deemed to "be despatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

(4) The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

(5) For the purposes of this section -

(i) if the originator or the addressee has more than one place of business, the principal place of business shall be the place of business;

(ii) if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business;

(iii)"Usual place of residence", in relation to a body corporate, means the place where it is registered.

4.8 SECURE ELECTRONIC RECORDS AND DIGITAL SIGNATURES

Chapter V sets out the conditions that would apply to qualify electronic records and digital signatures as being secure. It contains sections 14 to 16. Sections 14 to 16 deals with securing electronic records and electronic signatures.

Section 14 provides where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

In ITA 2000, Section 14 is given as follows:

[Section 14] Secure electronic record.

Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification.

Section 15 provides for the security procedure to be applied to digital signatures for being treated as a secure digital signature. It was substituted by ITAA 2008. This section states:

[Section 15] Secure Electronic Signature (Substituted vide ITAA 2008).

An electronic signature shall be deemed to be a secure electronic signature if-

(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed

Explanation - In case of digital signature, the "signature creation data" means the private key of the subscriber.

Section 16 provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures. In doing so, the Central Government shall take into account various factors like nature of the transaction, level of sophistication of the technological capacity of the parties, availability and cost of alternative procedures, volume of similar transactions entered into by other parties etc. This section was substituted by ITAA 2008. This section states:

[Section 16] Security procedures and Practices (Amended vide ITAA 2008).

The Central Government may for the purposes of sections 14 and 15 prescribe the security procedures and practices.

Provided that in prescribing such security procedures and practices, the Central Government shall have regard to the commercial circumstances, nature of transactions and such other related factors as it may consider appropriate.

4.9 SUMMARY

- Section 3 of the IT Act provides the conditions subject to which an electronic record may be authenticated by means of affixing digital signature. It gives legal validity to the use of digital signatures for authenticating documents.
- Section 3A of IT Act provides authentication of records by using any electronic signature or electronic authentication technique. If any alteration has been made to the electronic signature after affixing, it should be detectable.

4.1 Exercise

Exercise 1 : Mix and Match

signature is created in two distinct steps	retain and appropriate e-service charges by the service providers.
Subject to the provisions of sub-section (2), the appropriate Government may	Digital

authorize he service providers to collect, retain and appropriate service charges under this section notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect	
The appropriate Government shall, by notification in the Official Gazette, specify the scale of service charges which may be charged and collected by the	Provided that the appropriate Government
may specify different scale of service charges for different types of services.	service providers under this section:

Ans 1(2), 2(1), 3(4), 4(3)

Exercise 2: Fill in the blanks

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his………………….

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another……………..

(3) Any person by the use of a ………….of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a……………….

Ans. 1. Digital Signature 2. electronic record 3. public key 4. functioning key pair

Exercise 3: True / False

(a) Where the originator has stipulated that the acknowledgment of receipt of electronic record.

(b) Any communication by the addressee, automated or otherwise; or

(c) Any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.

(d) Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgment of such electronic record by him, then unless acknowledgment has been so received, the electronic record shall be deemed to have been never sent by the originator.

Ans. 1 False, 2. True 3. True 4. True.

Exercise 4 : Short Question Answers

(a) Explain Electronic Records Authentication of Electronic Records.

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

(b) Define Legal Recognition of Electronic Records.

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

(c) Explain Legal Recognition of Digital Signatures.

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

(d) Define Applications and usage of electronic records and Digital Signatures in Government and its Agencies.

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

(e) Explain Retention of Electronic Records.

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

………………………………………………………………………………………

(f) Define Intermediaries and their liabilities.

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

(g) Explain Attribution, Acknowledgement and Dispatch of Electronic Records.

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

(h) Define Secure Electronic Records and Digital Signatures.

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

…………………………………………………………………………………

Unit V

REGULATORY FRAMEWORK

- Regulatory Framework Regulation of Certifying Authorities;
- Appointment and Functions of Controller;
- License to issue Digital Signatures Certificate;
- Renewal of License;
- Controller’s Powers;
- Procedure to be Followed by Certifying Authority;
- Issue, Suspension and Revocation of Digital Signatures Certificate,
- Duties of Subscribers;
- Penalties and Adjudication;
- Appellate Tribunal;
- Offences;
- Overview of GDPR and Indian data protection regime
- Summary
- Exercise

5.1 REGULATION OF CERTIFYING AUTHORITIES

The success of sending and verifying secure digitally signed electronic message is contingent upon the presence of a robust infrastructure known as Public Key Infrastructure (PKI). A PKI consists of Certifying Authority; method of issuing, publishing, storing, revoking and archiving digital certificates; and interoperation between different Certifying Authorities. In many cases, a PKI consists of a trust hierarchy, where Certifying Authorities higher in the hierarchy proves the identity of the Certifying Authorities lower in the hierarchy. The Certifying Authority at the top of the hierarchy is generally known as root Certifying Authority.

Digital certificates are digitally signed electronic records, which verify that the holders of a public and private key are who they claim to be. The digital certificate contains subscriber’s name, his public key, name of Certifying Authority, date and time of issue and digital signature of the Certifying Authority, and provides a specific association with the private key. Trusted third party known as a Certifying Authority issues digital certificates. The Certifying Authority issues a digital certificate to each of the users, which provides the recipient with the confirmation that the public key used to sign the message was indeed issued to the sender. Digital certificates issued by the Certifying Authority are unforgeable because they are digitally signed with the private key of the Certifying Authority. The International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) recommendation X.509 governs the structure of the digital certificates.

Digital certificates can prove non-repudiation and confidentiality of the transaction. The receiver of message can store the transaction data along with the hash result and the Certifying Authority has a store of the digital signatures issues to a user so that if at a later date, the transaction is contested in the court, they can provide the digital certificates and the receiver can provide the transaction data and the original hash result. The transaction data and hash result can be computed with the signatures provided by the Certifying

Authority and matched with the hash result stored along with the transaction, to prove non-repudiation. The same signatures can also be used for encrypting transaction, on transaction medium, to ensure confidentiality of transaction.

Chapter VI contains detailed provisions relating to regulation of Certifying Authorities. It deals with the appointment and powers of the Controller and Certifying Authorities. It contains sections 17 to 34.

5.2 APPOINTMENT AND FUNCTIONS OF CONTROLLER

The provisions of appointment and functions of Controller are given in sections 17 to 19 of IT Act. They are discussed below:

5.2.1 Appointment of Controller and Other Officers

Section 17 of the IT Act provides for the appointment of Controller and other officers to regulate the Certifying Authorities. It empowers the Central Government to appoint the Controller of Certifying Authorities and other officers. As per Information Technology (Amendment) Act, 2008 (ITAA 2008), Section 17 is given as follows:

[Section 17] Appointment of Controller and other officers (Amended Vide ITAA 2008).

(1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers, other officers and employees (Inserted vide ITAA 2008) as it deems fit.

(2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.

(3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.

(4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers other officers and employees (Inserted vide ITAA 2008) shall be such as may be prescribed by the Central Government.

(5) The Head Office and Branch Office of the Office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(6) There shall be a seal of the Office of the Controller.

5.2.2 Functions of Controller

Section 18 of the IT Act lays down the functions, which the Controller may perform in respect of activities of Certifying Authorities. As per ITAA 2008, Section 18 is given as under:

[Section 18] Functions of Controller.

The Controller may perform all or any of the following functions, namely:

(a) exercising supervision over the activities of the Certifying Authorities;

(b) certifying public keys of the Certifying Authorities

(c) laying down the standards to be maintained by the Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

(e) specifying the conditions subject to which the Certifying Authorities shall conduct their business;

(f) specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of an electronic signature certificate and the Public Key;

(g) specifying the form and content of an electronic signature certificate and the key;

(h) specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

(i) specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;

(j) facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;

(k) specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;

(l) resolving any conflict of interests between the Certifying Authorities and the subscribers;

(m) laying down the duties of the Certifying Authorities;

(n) maintaining a data-base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

5.2.3 Recognition of Foreign Certifying Authorities by Controller

Section 19 of the IT Act provides for the power of the Controller with the previous approval of the Central Government to grant recognition to foreign Certifying Authorities subject to such conditions and restrictions as may be imposed by regulations. As per ITAA 2008, Section 19 is given as under:

[Section 19] Recognition of foreign Certifying Authorities.

(1) Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

(2) Where any Certifying Authority is recognized under sub-section (1), the electronic signature certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

(3) The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under

subsection (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.

5.3 LICENSE TO ISSUE DIGITAL SIGNATURE CERTIFICATES

Section 21 of the IT Act provides that a license to be issued to a Certifying Authority to issue digital signature certificates by the Controller shall be in such form and shall be accompanied with such fees and other documents as may be prescribed by the Central Government. Further, the Controller after considering the application may either grant the license or reject the application after giving reasonable opportunity of being heard. As per ITAA 2008, Section 21 is given as under:

[Section 21] License to issue electronic signature certificates.

(1) Subject to the provisions of sub-section (2), any person may make an application, to the Controller, for a license to issue electronic signature certificates.

(2) No license shall be issued under sub-section (1), unless the applicant fulfills such requirements with respect to qualification, expertise, manpower, financial resources and other infrastructure facilities, which are necessary to issue Electronic Signature

(3) Certificates as may be prescribed by the Central Government.

(4) A license granted under this section shall -

  (a) be valid for such period as may be prescribed by the Central Government;

  (b) not be transferable or heritable;

  (c) be subject to such terms and conditions as may be specified by the regulations.

Section 22 of the IT Act provides that the application for license shall be accompanied by a certification practice statement and statement including the procedure with respect to identification of the applicant. It shall be further accompanied by a fee not exceeding Rs.25,000 and other documents as may be prescribed by the Central Government. In ITAA 2008, section 22 is given as follows:

[Section 22] Application for license.

(1) Every application for issue of a license shall be in such form as may be prescribed by the Central Government.

(2) Every application for issue of a license shall be accompanied by-

  (a) a certification practice statement;

  (b) a statement including the procedures with respect to identification of the applicant;

  (c) payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

  (d) such other documents, as may be prescribed by the Central Government.

5.4 RENEWAL OF LICENSE

Section 23 of the IT Act provides that the application for renewal of a license shall be in such form and accompanied by such fees not exceeding Rs.5,000 which may be prescribed by the Central Government. In ITAA 2008, Section 23 is given as follows:

[Section 23] Renewal of license.

An application for renewal of a license shall be -

(a) in such form;

(b) accompanied by such fees, not exceeding five thousand rupees, as may be prescribed by the Central Government and shall be made not less than forty-five days before the date of expiry of the period of validity of the license.

5.5 CONTROLLER’S POWERS

The provisions of Controller’s powers are given in sections 24 to 29 of the IT Act. They are discussed below:

5.5.1 Procedure for Grant or Rejection of License by Controller

Section 24 of the IT Act deals with the procedure for grant or rejection of license by the controller on certain grounds. No application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case. In ITAA 2008, Section 24 is given as follows:

[Section 24] Procedure for grant or rejection of license.

The Controller may, on receipt of an application under sub-section (1) of section 21, after considering the documents accompanying the application and such other factors, as he deems fit, grant the license or reject the application:

However, no application shall be rejected under this section unless the applicant has been given a reasonable opportunity of presenting his case.

5.5.2 Suspension of License by Controller

Section 25 of the IT Act provides that the Controller may revoke a license on grounds such as incorrect or false material particulars being mentioned in the application and also on the ground of contravention of any provisions of the Act, rule, regulation or order made there under.

However, no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation. Also, no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

Thereafter, the Controller shall publish a notice of suspension or revocation of license as the case may be in the database maintained by him.

Further, the database containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock. It is also provided that the Controller may, if he considers necessary, publicize the contents of database in such electronic or other media, as he may consider appropriate. As per ITAA 2008, different sections are given as follows:

[Section 25] Suspension of license.

(1) The Controller may, if he is satisfied after making such inquiry, as he may think fit, that a Certifying Authority has -

   (a) made a statement in, or in relation to, the application for the issue or renewal of the license, which is incorrect or false in material particulars;

   (b) failed to comply with the terms and conditions subject to which the license was granted;

   (c) failed to maintain the standards specified in Section 30 [Substituted for the words "under clause (b) of sub-section (2) of section 20;" vide amendment dated September 19, 2002]

   (d) contravened any provisions of this Act, rule, regulation or order made there under, revoke the license:

   However, no license shall be revoked unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed revocation.

(2) The Controller may, if he has reasonable cause to believe that there is any ground for revoking a license under sub-section (1), by order suspend such license pending the completion of any enquiry ordered by him:

   However, no license shall be suspended for a period exceeding ten days unless the Certifying Authority has been given a reasonable opportunity of showing cause against the proposed suspension.

(3) No Certifying Authority whose license has been suspended shall issue any electronic signature certificate during such suspension.

5.5.3 Notice of Suspension or Revocation of License by Controller

Section 26 of the IT Act provides for the notice of suspension or revocation of license by the Controller. It is given below:

[Section 26] Notice of suspension or revocation of license.

(1) Where the license of the Certifying Authority is suspended or revoked, the Controller shall publish notice of such suspension or revocation, as the case may be, in the database maintained by him.

(2) Where one or more repositories are specified, the Controller shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

However, the data-base containing the notice of such suspension or revocation, as the case may be, shall be made available through a web site which shall be accessible round the clock However, that the Controller may, if he considers necessary, publicize the contents of the data-base in such electronic or other media, as he may consider appropriate.

5.5.4 Controller’s Power to Delegate

Section 27 of the IT Act contains provisions for the delegation of powers by the Controller. It is given below:

[Section 27] Power to delegate.

The Controller may, in writing, authorize the Deputy Controller, Assistant Controller or any officer to exercise any of the powers of the Controller under this Chapter.

The Controller or any person authorized by him, shall have access to any computer system, data or any other material connected with such system if he has reasonable cause to suspect that contravention of the provisions of the Act or the rules or regulation is being committed.

5.5.4 Controller's Power to Investigate Contraventions

Section 28 of the IT Act contains provisions regarding the powers available to Controller to investigate contraventions. The powers available to Controller are similar to powers of Income-tax authorities under Chapter XIII of the Income Tax Act, 1961. Section 28 is given below:

[Section 28] Power to investigate contraventions.

(1) The Controller or any officer authorized by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made there under.

(2) The Controller or any officer authorized by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income Tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.

5.5.5 Access of Computers and Data to Controller

Section 29 of the IT Act contains provisions regarding powers of Controller to access computers and data. It is given below:

[Section 29] Access to computers and data.

(1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this chapter made there under has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system. (Amended vide ITAA 2008)

(2) For the purposes of sub-section (1), the Controller or any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of the computer system, data apparatus or material, to provide him with such reasonable technical and other assistant as he may consider necessary.

5.6 ISSUE, SUSPENSION AND REVOCATION OF DIGITAL SIGNATURE CERTIFICATES

Chapter VII of the IT Act deals with digital or electronic signature certificates. It should be noted that ITAA 2008 substituted the word "electronic signature" in place of "digital signature". Sections 35 to 39 of the IT Act contains provisions regarding issue, suspension and revocation of electronic signature certificates. They are discussed below:

5.6.1 Certifying Authority to Issue Digital Signature Certificate

Section 35 of the IT Act lays down the procedure for issuance of a digital signature certificate. It provides that an application for such certificate shall be made in the prescribed form and shall be accompanied by a fee not exceeding Rs.25,000. The fee shall be prescribed by the Central Government, and different fees may be prescribed for different classes of applicants.

The section also provides that no digital signature certificate shall be granted unless the Certifying Authority is satisfied that –

(a) the applicant holds the private key corresponding to the public key to be listed in the digital signature certificate;

(b) the applicant holds a private key, which is capable of creating a digital signature;

(c) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the applicant.

However, no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

(1) Any person may make an application to the Certifying Authority for the issue of a digital signature certificate in such form as may be prescribed by the Central Government.

(2) Every such application shall be accompanied by such fee not exceeding twenty-five thousand rupees as may be prescribed by the Central Government, to be paid to the Certifying Authority:

However, while prescribing fees under sub-section (2) different fees may be prescribed for different classes of applicants.

(3) Every such application shall be accompanied by a certification practice statement or where there is no such statement, a statement containing such particulars, as may be specified by regulations.

(4) On receipt of an application under sub-section (1), the Certifying Authority may, after consideration of the certification practice statement or the other statement under sub-section and after making such enquiries as it may deem fit, grant the digital signature certificate or for reasons to be recorded in writing, reject the application

However, no application shall be rejected unless the applicant has been given a reasonable opportunity of showing cause against the proposed rejection.

5.6.2 Representations upon Issuance of Digital Signature Certificate

Section 36 of the IT Act requires that while issuing a digital signature certificate, the Certifying Authority should certify that it has complied with the provisions of the Act, the rules and regulations made there under and also with other conditions mentioned in the digital signature certificate. It is given below:

[Section 36] Representations upon issuance of digital signature certificate.

A Certifying Authority while issuing a digital signature certificate shall certify that -

(a) it has complied with the provisions of this Act and the rules and regulations made there under;

(b) it has published the digital signature certificate or otherwise made it available to such person relying on it and the subscriber has accepted it;

(c) the subscriber holds the private key corresponding to the public key, listed in the digital signature certificate;

(ca) the subscriber holds a private key which is capable of creating a digital signature (Inserted vide ITAA 2008)

(cb) the public key to be listed in the certificate can be used to verify a digital signature affixed by the private key held by the subscriber (Inserted vide ITAA 2008)

(d) the subscriber's public key and private key constitute a functioning key pair;

(e) the information contained in the digital signature certificate is accurate; and

(f) it has no knowledge of any material fact, which if it had been included in the digital signature certificate would adversely affect the reliability of the representations made in clauses (a) to (d).

5.6.3 Suspension of Digital Signature Certificate

Section 37 of the IT Act contains provisions regarding suspension of digital signature certificate. It is given below:

[Section 37] Suspension of digital signature certificate.

The Certifying Authority may suspend such certificate if it is of the opinion that such a step needs to be taken in public interest.

Such certificate shall not be suspended for a period exceeding 15 days unless the subscriber has been given an opportunity of being heard.

Subject to the provisions of sub-section (2), the Certifying Authority which has issued a digital signature certificate may suspend such digital signature certificate -

(a) on receipt of a request to that effect from -

(i) the subscriber listed in the digital signature certificate; or

(ii) any person duly authorized to act on behalf of that subscriber;

(b) if it is of opinion that the digital signature certificate should be suspended in public interest

A digital signature certificate shall not be suspended for a period exceeding fifteen days unless the subscriber has been given an opportunity of being heard in the matter.

On suspension of a digital signature certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

5.6.4 Revocation of Digital Signature Certificate

Section 38 of the IT Act provides for the revocation of digital signature certificates under certain circumstances. Such revocation shall not be done unless the subscriber has been given an opportunity of being heard in the matter. Upon revocation or suspension the certifying Authority shall publish the notice of suspension or revocation of a digital signature certificate. This section states that –

[Section 38] Revocation of digital signature certificate.

A Certifying Authority may revoke a digital signature Certificate issued by it

(a) where the subscriber or any other person authorized by him makes a request to that effect; or

(b) upon the death of the subscriber; or

(c) upon the dissolution of the firm or winding up of the company where the subscriber is a firm or a company.

Subject to the provisions of sub-section (3) and without prejudice to the provisions of sub-section(1), a Certifying Authority may revoke a digital signature certificate which has been issued by it at any time, if it is of opinion that -

(a) a material fact represented in the digital signature certificate is false or has been concealed;

(b) a requirement for issuance of the digital signature certificate was not satisfied;

(c) the Certifying Authority's private key or security system was compromised in a manner materially affecting the digital signature certificate's reliability;

(d) the subscriber has been declared insolvent or dead or where a subscriber is a firm or a company, which has been dissolved, wound-up or otherwise ceased to exist.

A digital signature certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

On revocation of a digital signature certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

5.6.5 Notice of Suspension or Revocation of Digital Signature Certificate

Section 39 of the IT Act contains requirements regarding publication of notice of suspension or revocation of digital signature certificate. It is given below:

[Section 39] Notice of suspension or revocation.

(1) Where a digital signature certificate is suspended or revoked under section 37 or section 38, the Certifying Authority shall publish a notice of such suspension or revocation, as the case may be, in the repository specified in the digital signature certificate for publication of such notice.

(2) Where one or more repositories are specified, the Certifying Authority shall publish notices of such suspension or revocation, as the case may be, in all such repositories.

5.7 CYBER APPELLATE TRIBUNAL

The Cyber Appellate Tribunal has appellate powers in respect of orders passed by any adjudicating officer. Civil courts have been barred from entertaining any suit or proceeding in respect of any matter which an adjudicating officer or Tribunal is empowered to handle.

The provisions related to Cyber Appellate Tribunal are given in sections 48 to 62 of the IT Act. They are discussed below:

5.7.1 Establishment of Cyber Appellate Tribunal

Section 48 of the IT Act provides for establishment of one or more Appellate Tribunals to be known as Cyber Regulations Appellate Tribunals.

The Cyber Regulations Appellate Tribunal shall consist of one person only (called the Presiding Officer of the Tribunal) who shall be appointed by notification by the Central Government. Such a person must be qualified to be a judge of a High Court or is or has been a member of the Indian Legal Service in the post in Grade I of that service for at least three years.

The Presiding Officer shall hold office for a term of five years or up to a maximum age limit of 65 years, whichever is earlier. As per ITAA 2008 different sections are given as follows:

[Section 48] Establishment of Cyber Appellate Tribunal.

(1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction.

5.7.2 Composition of Cyber Appellate Tribunal

Section 49 of the IT Act contains provisions regarding composition of Cyber Appellate Tribunal. It is given below:

[Section 49] Composition of Cyber Appellate Tribunal (Substituted vide ITAA 2008).

(1) The Cyber Appellate Tribunal shall consist of a Chairperson and such number of other Members, as the Central Government may, by notification in the Official Gazette, appoint (Inserted vide ITAA-2008).

Provided that the person appointed as the Presiding Officer of the Cyber Appellate Tribunal under the provisions of this Act immediately before the commencement of the Information Technology (Amendment) Act 2008 shall be deemed to have been appointed as the Chairperson of the said Cyber Appellate Tribunal under the provisions of this Act as amended by the Information Technology (Amendment) Act, 2008 (Inserted vide ITAA 2008).

(2) The selection of Chairperson and Members of the Cyber Appellate Tribunal shall be made by the Central Government in consultation with the Chief Justice of India. (Inserted vide ITAA-2008).

(3) Subject to the provisions of this Act-

(a) the jurisdiction, powers and authority of the Cyber Appellate Tribunal may be exercised by the Benches thereof

(b) a Bench may be constituted by the Chairperson of the Cyber Appellate Tribunal with one or two members of such Tribunal as the Chairperson may deem fit.

Provided that every Bench shall be presided over by the Chairperson or the Judicial Member appointed under sub-section (3) of section 50 (ITAA 2008)

(c) the Benches of the Cyber Appellate Tribunal shall sit at New Delhi and at such other places as the Central Government may, in consultation with the Chairperson of the Cyber Appellate Tribunal, by notification in the Official Gazette, specify.

(d) the Central Government shall, by notification in the Official Gazette, specify the areas in relation to which each Bench of the Cyber Appellate Tribunal may exercise its jurisdiction. (Inserted vide ITAA-2008).

(4) Notwithstanding anything contained in sub-section (3), the Chairperson of the Cyber Appellate Tribunal may transfer a Member of such Tribunal from one Bench to another Bench (Inserted vide ITAA-2008)

(5) If at any stage of the hearing of any case or matter, it appears to the Chairperson or a Member of the Cyber Appellate Tribunal that the case or matter is of such a nature that it ought to be heard by a Bench consisting of more Members, the case or matter may be transferred by the Chairperson to such Bench as the Chairperson may deem fit. (Inserted vide ITAA-2008)

5.7.3 Qualifications for Appointment as Chairperson and Members of Cyber Appellate Tribunal

Section 50 of the IT Act deals with qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal. It is given below:

[Section 50] Qualifications for appointment as Chairperson and Members of Cyber Appellate Tribunal (Substituted vide ITAA 2008).

(1) A person shall not be qualified for appointment as a Chairperson of the Cyber Appellate Tribunal unless he is, or has been, or is qualified to be, a Judge of a High Court; (substituted vide ITAA-2008)

(2) The Members of the Cyber Appellate Tribunal, except the Judicial Member to be appointed under sub-section (3), shall be appointed by the Central Government from amongst persons, having special knowledge of and professional experience in, information technology, telecommunication, industry, management or consumer affairs.

Provided that a person shall not be appointed as a Member, unless he is, or has been, in the service of the Central Government or a State Government, and has held the post of Additional secretary to the Government of India or any equivalent post in the Central Government or State Government for a period of not less than two one years or joint secretary to the Government of India or any equivalent post in the central Government or State Government for a period of not less than seven years. (Inserted vide ITAA-2008)

(3) The Judicial Members of the Cyber Appellate Tribunal shall be appointed by the Central Government from amongst persons who is or has been a member of the Indian Legal Service and has held the post of Additional Secretary for a period of

not less than one year or Grade I post of that service for a period of not less than five years.

5.7.4 Term of Office and Conditions of Service of Chairperson and Members of Cyber Appellate Tribunal

Section 51 of the IT Act contains provisions regarding the term of office, conditions of service etc. of Chairperson and Members of Cyber Appellate Tribunal. It is given below:

[Section 51] Term of office, conditions of service etc. of Chairperson and Members (Substituted vide ITAA 2008).

(1) The Chairperson or Member of the Cyber Appellate Tribunal shall hold office for a term of five years from the date on which he enters upon his office or until he attains the age of sixty-five years, whichever is earlier. (Inserted vide ITAA 2008)

(2) Before appointing any person as the Chairperson or Member of the Cyber Appellate Tribunal, the Central Government shall satisfy itself that the person does not have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member. (Inserted vide ITAA 2008)

(3) An officer of the Central Government or State Government on his selection as the Chairperson or Member of the Cyber Appellate Tribunal, as the case may be, shall have to retire from service before joining as such Chairperson or Member. (Inserted vide ITAA 2008).

5.7.5 Salary, Allowance and Other Terms and Conditions of Service of Chairperson and Members of Cyber Appellate Tribunal

Section 52 of the IT Act provides for the salary and allowances and other terms and conditions of service of the presiding Officer of Cyber Appellate Tribunal. It is given below:

[Section 52] Salary, allowance and other terms and conditions of service of Chairperson and Member (Substituted vide ITAA 2008).

The salary and allowances payable to, and the other terms and conditions of service including pension, gratuity and other retirement benefits of, the Chairperson or a Member of Cyber Appellate Tribunal shall be such as may be prescribed. (Inserted vide ITAA 2008)

Section 52A of the IT Act deals with powers of superintendence and direction of Chairperson of the Cyber Appellate Tribunal. It is given below:

[Section 52A] Powers of superintendence, direction, etc. (Inserted vide ITAA 2008).

The Chairperson of the Cyber Appellate Tribunal shall have powers of general superintendence and directions in the conduct of the affairs of that Tribunal and he shall, in addition to presiding over the meetings of the Tribunal, exercise and discharge such powers and functions of the Tribunal as may be prescribed.

Section 52B of the IT Act deals with distribution of business among benches of Cyber Appellate Tribunal by the Chairperson. It is given below:

[Section 52B] Distribution of Business among Benches (Inserted vide ITAA 2008).

Where Benches are constituted, the Chairperson of the Cyber Appellate Tribunal may, by order, distribute the business of that Tribunal amongst the Benches and also the matters to be dealt with by each Bench.

Section 52C of the IT Act deals with powers of Chairperson of the Cyber Appellate Tribunal to transfer cases. It is given below:

[Section 52C] Powers of the Chairperson to transfer cases (Inserted vide ITAA 2008).

On the application of any of the parties and after notice to the parties, and after hearing such of them as he may deem proper to be heard, or suo moto without such notice, the Chairperson of the Cyber Appellate Tribunal may transfer any case pending before one Bench, for disposal to any other Bench.

Section 52D of the IT Act contains provisions regarding decision of the Cyber Appellate Tribunal by majority. It is given below:

[Section 52D] Decision by majority (Inserted vide ITAA 2008).

If the Members of a Bench consisting of two Members differ in opinion on any point, they shall state the point or points on which they differ, and make a reference to the Chairperson of the Cyber Appellate Tribunal who shall hear the point or points himself and such point or points shall be decided according to the opinion of the majority of the Members who have heard the case, including those who first heard it.

5.7.6 Filling up of Vacancies of Cyber Appellate Tribunal

Section 53 of the IT Act provides that in the situation of any vacancy occurring in the office of the Presiding officer of Cyber Regulations Tribunal, the Central Government shall appoint another person in accordance with the provisions of this Act.

[Section 53] Filling up of vacancies (Amended vide ITAA 2008).

If, for reason other than temporary absence, any vacancy occurs in the office of the Chairperson or Member as the case may be of a Cyber Appellate Tribunal, then the Central Government shall appoint another person in accordance with the provisions of this Act to fill the vacancy and the proceedings may be continued before the Cyber Appellate Tribunal from the stage at which the vacancy is filled.

5.7.7 Resignation and Removal of Chairperson and Members of the Cyber Appellate Tribunal

Section 54 of the IT Act contains provisions regarding the resignation and removal of Chairperson and Members of the Cyber Appellate Tribunal. It is given below:

[Section 54] Resignation and removal (Amended vide ITAA 2008).

(1) The Chairperson or Member of the Cyber Appellate Tribunal may, by notice in writing under his hand addressed to the Central Government, resign his office:

    However, the said Chairperson or Member shall, unless he is permitted by the Central Government to relinquish his office sooner, continue to hold office until the expiry of three months from the date of receipt of such notice or until a person duly appointed as his successor enters upon his office or until the expiry of his term of office, whichever is the earliest.

(2) The Chairperson or Member of a Cyber Appellate Tribunal shall not be removed from his office except by an order by the Central Government on the ground of proved misbehavior or incapacity after an inquiry made by a Judge of the Supreme Court in which the Chairperson or Member concerned has been informed of the charges against him and given a reasonable opportunity of being heard in respect of these charges.

(3) The Central Government may, by rules, regulate the procedure for the investigation of misbehavior or incapacity of the aforesaid Chairperson or Member.

5.7.8 Orders Constituting Cyber Appellate Tribunal

Section 55 of the IT Act contains provisions regarding orders constituting Cyber Appellate Tribunal. It is given below:

[Section 55] Orders constituting Appellate Tribunal to be final and not to invalidate its proceedings (Inserted vide ITAA 2008).

No order of the Central Government appointing any person as the Chairperson or Member of a Cyber Appellate Tribunal shall be called in question in any manner and no act or proceeding before a Cyber Appellate Tribunal shall be called in question in any manner on the ground merely of any defect in the constitution of a Cyber Appellate Tribunal.

5.7.9 Staff of the Cyber Appellate Tribunal

Section 56 of the IT Act contains provisions regarding staff of the Cyber Appellate Tribunal. It is given below:

[Section 56] Staff of the Cyber Appellate Tribunal.

(1) The Central Government shall provide the Cyber Appellate Tribunal with such officers and employees as the Government may think fit.

(2) The officers and employees of the Cyber Appellate Tribunal shall discharge their functions under general superintendence of the Presiding Officer.

(3) The salaries and allowances and other conditions of service of the officers and employees of the Cyber Appellate Tribunal shall be such as may be prescribed by the Central Government.

5.7.10 Appeal to Cyber Appellate Tribunal

Section 57 of the IT Act contains provisions regarding appeal to Cyber Appellate Tribunal. It is given below:

[Section 57] Appeal to Cyber Appellate Tribunal.

(1) Save as provided in sub-section (2), any person aggrieved by an order made by a Controller or an adjudicating officer under this Act may prefer an appeal to a Cyber Appellate Tribunal having jurisdiction in the matter

(2) No appeal shall lie to the Cyber Appellate Tribunal from an order made by an adjudicating officer with the consent of the parties.

(3) Every appeal under sub-section (1) shall be filed within a period of forty-five days from the date on which a copy of the order made by the Controller or adjudicating officer is received by the person aggrieved and it shall be in such form and be accompanied by such fee as may be prescribed:

However, the Cyber Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appeal under sub-section (1), the Cyber Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against

(5) The Cyber Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the concerned Controller or adjudicating officer.

(6) The appeal filed before the Cyber Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavor shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal.

5.7.11 Procedure and Powers of the Cyber Appellate Tribunal

Section 58 of the IT Act contains provisions regarding procedure and powers of Cyber Appellate Tribunal. It is given below:

[Section 58] Procedure and Powers of the Cyber Appellate Tribunal.

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2) The Cyber Appellate Tribunal shall have, for the purposes of discharging their functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely -

(a) summoning and enforcing the attendance of any person and examining him on oath;

(b) requiring the discovery and production of documents or other electronic records;

(c) receiving evidence on affidavits;

(d) issuing commissions for the examination of witnesses or documents;

(e) reviewing its decisions;

(f) dismissing an application for default or deciding it ex parte

(g) any other matter which may be prescribed

Every proceeding before the Cyber Appellate Tribunal shall be deemed .to be a judicial proceeding within the meaning of sections 193 arid 228, and for the purposes of section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973.

5.7.12 Right to Legal Representation before Cyber Appellate Tribunal

Section 59 of the IT Act contains provisions regarding legal representation before Cyber Appellate Tribunal. It is given below:

[Section 59]: Right to legal representation.

The appellant may either appear in person or authorize one or more legal practitioners or any of its officers to present his or its case before the Cyber Appellate Tribunal.

5.7.13 Limitation Act 1963 to Apply to Appeals to Cyber Appellate Tribunal

Section 60 of the IT Act states the provisions of Limitation Act, 1963 to would apply to appeals before Cyber Appellate Tribunal. It is given below:

[Section 60] Limitation.

The provisions of the Limitation Act, 1963, shall, as far as may be, apply to an appeal made to the Cyber Appellate Tribunal.

5.7.14 Bar on Jurisdiction of Civil Courts

Section 61 of the IT Act places bar on the jurisdiction of civil courts in matters where adjudicating officer appointed or the Cyber Appellate Tribunal is constituted under IT Act. It is given below:

[Section 61] Civil court not to have jurisdiction (Amended vide ITAA 2008).

No court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which an adjudicating officer appointed under this Act or the Cyber Appellate Tribunal constituted under this Act is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

Provided that the court may exercise jurisdiction in cases where the claim for injury or damage suffered by any person exceeds the maximum amount which can be awarded under this Chapter. (Inserted vide ITAA 2008).

5.7.15 Appeal to High Court against Decision of Cyber Appellate Tribunal

Section 62 of the IT Act contains provisions regarding appeal to High Court against decision of Cyber Appellate Tribunal. It is given below:

[Section 62] Appeal to High Court.

Any person aggrieved by any decision or order of the Cyber Appellate Tribunal may file an appeal to the High Court within sixty days from the date of communication of the decision or order of the Cyber Appellate Tribunal to him on any question of fact or law arising out of such order:

However, the High Court may, if it is satisfied that the appellant was prevented by sufficient cause from filing the appeal within the said period, allow it to be filed within a further period not exceeding sixty days.

5.8 OFFENCES

Chapter XI deals with some computer crimes and provides for penalties for these offences. It contains sections 65 to 78. They are discussed below:

5.8.1 Tampering with Computer Source Documents

Section 65 of the IT Act provides for punishment up to three years or with a fine which may extend to Rs. 2 lakhs or with both whoever knowingly or intentionally tampers with the computer code source documents.

“Computer source code” means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. As per ITAA 2008, Section 65 is given as follows:

[Section 65] Tampering with computer source documents.

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation - For the purposes of this section, "Computer Source Code" means the listing of programmes, Computer Commands, Design and layout and programme analysis of computer resource in any form.

5.8.2 Computer Related Offences

Section 66 of the IT Act deals with computer related offences like hacking. ‘Hacking’ was a term defined in Information Technology Act, 2000 (ITA 2000). It was used to describe the act of destroying or deleting or altering any information residing in a computer resource or diminishing its value or utility, or affecting it injuriously in spite of knowing that such action is likely to cause wrongful loss or damage to the public or that person. Section 66 provided that a person who commits hacking shall be punished with a fine up to Rs.2 lakhs or with imprisonment up to 3 years, or with both. This section of ITA 2000 was replaced by ITA 2008. As per ITAA 2008, Section 66 is given as follows:

[Section 66] Computer Related Offences (Substituted vide ITAA 2008).

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.

Explanation: For the purpose of this section,-

(a) the word "dishonestly" shall have the meaning assigned to it in section 24 of the Indian Penal Code;

(b) the word "fraudulently" shall have the meaning assigned to it in section 25 of the Indian Penal Code.

Section 43 of the IT Act deals with penalties for damage to computer, computer system, etc. It is given below:

[Section 43] Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is in-charge of a computer, computer system or computer network, —

(a) accesses or secures access to such computer, computer system or computer network;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network,

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means (inserted vide ITAA 2008)

(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage, (inserted vide ITAA 2008)

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation — For the purposes of this section,—

(i) "computer contaminant" means any set of computer instructions that are designed—

  (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

  (b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(ii) "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

(iii) "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

(v) "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form (Inserted vide ITAA 2008)

Section 66A of the IT Act dealt with punishment for sending offensive messages through communication service. This section has been declared unconstitutional by the Supreme Court of India. This section had been widely misused by police in various states to arrest innocent persons for posting critical comments about social and political issues and political leaders on social networking sites. The court said that this section hit at the root of liberty and freedom of expression, two cardinal pillars of democracy. The Supreme Court said section 66A was vaguely worded and allowed its misuse by police. As per the direction of the court, section 66A had to be erased from the law books as it has gone much beyond the reasonable restrictions put by the Constitution on freedom of speech.

Section 66B of the IT Act deals with punishment for dishonestly for receiving stolen computer resource or communication device. It is given below:

[Section 66B] Punishment for dishonestly for receiving stolen computer resource or communication device (Inserted Vide ITAA 2008).

Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C of the IT Act contains provisions regarding punishment for identity theft. It is given below:

[Section 66C] Punishment for identity theft (Inserted vide ITAA 2008).

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D of the IT Act deals with punishment for cheating by personation by using computer resource. Personation is the act of assuming the character of another person without lawful authority, and, in such character, doing something to his prejudice, or to the prejudice of another, without his will or consent. It is given below:

[Section 66D] Punishment for cheating by personation by using computer resource (Inserted vide ITAA 2008).

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E of the IT Act deals with punishment for violation of privacy. It is given below:

[Section 66E] Punishment for violation of privacy (Inserted vide ITAA 2008).

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Explanation - For the purposes of this section -

(a) "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) "capture", with respect to an image, means to videotape, photograph, film or record by any means;

(c) "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

(d) "publishes" means reproduction in the printed or electronic form and making it available for public;

(e) "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that--

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Section 66F of the IT Act deals with punishment for cyber terrorism. It is given below:

[Section 66F] Punishment for cyber terrorism (Inserted Vide ITAA 2008).

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any computer contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70, or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

5.8.3 Publishing of Obscene Information in Electronic Form

Section 67 of the IT Act provides for punishment to whoever transmits or publishes or causes to be published or transmitted, any material which is obscene in electronic form with imprisonment for a term which may extend to five years and with fine which may extend to Rs.1 lakh on first conviction. In the event of second or subsequent conviction the imprisonment would be for a term which may extend to ten years and fine which may extend to Rs. 2 lakhs. As per ITAA 2008, Section 67 is given as under:

[Section 67] Punishment for publishing or transmitting obscene material in electronic form (Amended vide ITAA 2008).

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67A of the IT Act deals with punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form. It is given below:

[Section 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form (Inserted vide ITAA 2008).

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Exception: This section and section 67 does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting, representation or figure is in the interest of science, literature, art, or learning or other objects of general concern; or

(ii) which is kept or used bona fide for religious purposes.

Section 67B of the IT Act deals with punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form. It is given below:

[Section 67B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.

Whoever,-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or

(d) facilitates abusing children online or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form-

(i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bonafide heritage or religious purposes.

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Section 67C of the IT Act deals with preservation and retention of information by intermediaries. It is given below:

[Section 67C] Preservation and Retention of information by intermediaries.

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

5.8.4 Power of Controller to give Directions

Section 68 of the IT Act provides that the controller may give directions to a Certifying Authority or any employee of such authority to take such measures or cease carrying on such activities as specified in the order, so as to ensure compliance with this law. If any person fails to comply, he shall be liable to imprisonment up to 3 years or fine up to Rs.2 lakhs, or both. As per ITAA 2008, Section 68 is given as under:

[Section 68] Power of Controller to give directions (Amended Vide ITAA 2008).

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who intentionally or knowingly (Inserted vide ITAA 2008) fails to comply with any order under sub-section (1) shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding two years or to a fine not exceeding one lakh rupees or to both.

5.8.5 Penalty for Misrepresentation

Section 71 of the IT Act provides that any person found misrepresenting or suppressing any material fact from the Controller or the Certifying Authority shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both. As per ITAA 2008, Section 71 is given as follows:

[Section 71] Penalty for misrepresentation.

Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or electronic signature certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

5.8.6 Breach of Confidentiality and Privacy

Section 72 of the IT Act provides a punishment for breach of confidentiality and privacy of electronic records, books, information, etc. by a person who has access to them without the consent of the person to whom they belong with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both. As per ITAA 2008, Section 72 is given as under:

[Section 72] Breach of confidentiality and privacy.

Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72A of the IT Act deals with punishment for disclosure of information in breach of lawful contract. It is given as under:

[Section 72A] Punishment for Disclosure of information in breach of lawful contract (Inserted vide ITAA-2008).

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both.

5.8.7 Penalty for Publishing False Electronic Signature Certificate

Section 73 of the IT Act provides punishment for publishing a digital signature certificate false in material particulars or otherwise making it available to any other person with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both. As per ITAA 2008, Section 73 is given as follows:

[Section 73] Penalty for publishing electronic signature certificate false in certain particulars.

(1) No person shall publish an electronic signature certificate or otherwise make it available to any other person with the knowledge that

  (a) the Certifying Authority listed in the certificate has not issued it; or

  (b) the subscriber listed in the certificate has not accepted it; or

  (c) the certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

5.8.8 Publication for Fraudulent Purpose

Section 74 of the IT Act provides for punishment with imprisonment for a term which may extend to two years or with fine which may extend to Rs.1 lakh or with both to a person whoever knowingly publishes for fraudulent purpose any digital signature certificate. As per ITAA 2008, section 74 is given as follows:

[Section 74] Publication for fraudulent purpose.

Whoever knowingly creates, publishes or otherwise makes available an electronic signature certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

5.8.9 Extra-Territorial Effect of IT Act

The application of the Act and its extra-territorial effect can be well understood by a conjoint reading of sections 1, 75 and 81. The IT Act extends to the whole of India. It applies also to any offence or contravention thereunder committed outside India by any person. However, an exception to this rule has been carved out in section 75 of the Act. Sub-section (1) of section 75 though in wider terms has made the Act applicable also to any offence or contravention committed outside India by any person irrespective of his nationality, this sub-section has been made subject to the provisions of sub-section (2) which states that for the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network in India. In effect, if an act (amounting to an offence under the Act) has been committed and where any computer, computer system or computers which are interconnected to each other in a computer network and which is in India is also involved (which might be either as a tool for committing the crime or as a target to the crime), then the provisions of the Act would apply to such an act. Section 81 provides effect to the provisions of the Act notwithstanding anything inconsistent contained in any other law for the time being in force. Therefore, effectively even if an offence (falling under the Act) is committed outside India by a foreigner, yet the courts in India would have the jurisdiction.

It is noticeable that with the IT Act, there has been a conceptual change with regard to the applicability of a statute. Due to the borderless connectivity of the computers through the Internet, and the ease with which one can commit a cyber-crime in India while physically located beyond the boundaries of the country, the Parliament has made the provisions of the Act applicable irrespective of where the accused might be physically located. In contrast, if we see the extent of operation of the Indian Penal Code (IPC) under section 1, it extends only ‘to the whole of India except the State of Jammu and Kashmir’. No further applicability clause has been provided for. Section 2 of the IPC makes every person including a foreigner liable to punishment for every act or omission contrary to the provisions of IPC, of which he/she shall be guilty in India. Sections 3 and 4 of the IPC relate to the extra-territorial operation of the Code. But these sections too are restrictive in nature and not as broad as the combined effect of section 1(2) read with section 75 of the IT Act.

5.8.10 Confiscation of Computer Related Equipment’s

Section 76 of the IT Act provides for confiscation of any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto in respect of contravention of any provision of the Act, rules, regulations or orders made there under.

It is also provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening the provisions of this Act, rules, orders or regulations made there under as it may think fit. Section 76 is as under:

[Section 76] Confiscation.

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

However, where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

5.8.11 Non-interference of Compensation, Penalties and Confiscation with Other Punishments

Section 77 of the IT Act further provides that penalty and confiscation provided under this Act shall not interfere with other punishments provided under any other law for the time being in force.

Different parts of Section 77 is as follows:

[Section 77] Compensation, penalties or confiscation not to interfere with other punishment (Substituted Vide ITAA-2008).

No compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force. Different subsections of the section is given as follows:

Section 77A of the IT Act deals with compounding of offences. It is given below:

[Section 77A] Compounding of Offences.

(1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.

Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265 C of Code of Criminal Procedures, 1973 shall apply.

Section 77B of the IT Act provides that offences with three year or above punishment will be cognizable. Cognizable offence means an offence wherein a police officer can arrest without warrant. Non-cognizable offence means a police officer does not have the authority to make an arrest without a warrant and an investigation cannot be initiated without a court order. In cognizable offences, there are certain provisions such as:

- The police is also allowed to start an investigation with or without the permission of a court.
- The police can file a First Information Report (FIR) only in cases of cognizable offences.
- The Supreme Court of India said it is mandatory for the police to register a FIR for all complaints in which cognizable offence has been discovered.

Further section 77B of the IT Act states that the offences punishable with three year imprisonment shall be bailable. In case of bailable offence, the grant of bail is a matter of right. It may be either given by a police officer who is having the custody of accused or by the court. The accused may be released on bail, on executing a “bail bond", with or without furnishing sureties.

The "bail bond" may contain certain terms and conditions, such as:

- The accused will not leave the territorial jurisdiction of the state without permission of court or police officer.
- The accused shall give his presence before police officer every time, he is required to do so.
- The accused will not tamper with any evidence whatsoever, considered by police in the investigation.

The court is empowered to refuse bail to an accused person even if the offence is bailable, where the person granted bail fails to comply with the conditions of the bail bond.

A non-bailable offence is one in which the grant of bail is not a matter of right. Here the accused will have to apply to the court, and it will be the discretion of the court to grant bail or not.

5.8.12 Police Officer Empowered to Investigate Offences

Section 78 of the IT Act provides for power to investigate the offences under the Act by a police officer not below the rank of Deputy Superintendent of Police. This is as follows:

[Section 78] Power to investigate offences (Amended Vide ITAA 2008).

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Inspector shall investigate any offence under this Act. (Amended Vide ITAA 2008)

5.9 OVERVIEW OF GDPR AND INDIAN DATA PROTECTION REGIME

General Data Protection Regulation (GDPR). In allowing global digital companies to work under certain conditions like:

1. National Interest
2. Confidentially of the data
3. Sovereignty and many more

Indian Data Protection Regime (DPR) is working on the confidentiality of the data of Indian citizens. They are also planning for Data Protection Authority for this. A Bill on Data Protection Bill 2019 also introduced.

5.10 SUMMARY

- A Public Key Infrastructure (PKI) consists of Certifying Authority; method of issuing, publishing, storing, revoking and archiving digital certificates; and interoperation between different Certifying Authorities.
- Digital certificates are digitally signed electronic records, which verify that the holders of a public and private key are who they claim to be. They can prove non-repudiation and confidentiality of the transaction.
- Section 17 of the IT Act provides for the appointment of Controller and other officers to regulate the Certifying Authorities.

5.11 EXERCISE

Exercise 1 : Mix and Match

consists of Certifying Authority; method of issuing, publishing, storing, revoking and archiving digital certificates; and interoperation between different Certifying Authorities.	Digital certificates are digitally signed
electronic records, which verify that the holders of a public and private key are who they claim to be. They can prove non-repudiation and confidentiality of the transaction.	A Public Key Infrastructure (PKI)
is working on the confidentiality of the data of Indian citizens.	Public Key Infrastructure (PKI)
The success of sending and verifying secure digitally signed electronic message is contingent upon the presence of a robust infrastructure known as	Indian Data Protection Regime (DPR)

Ans 1. (2), 2(1), 3 (4), 4(3)

Exercise 2 : Fill in the blanks

(1) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the ………………..

(2) The qualifications, experience and terms ………………..Deputy Controllers and Assistant Controllers other officers and employees (Inserted vide ITAA 2008) shall be such as may be prescribed by the Central Government.

(3) …………………of the Office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.

(4) There shall be a seal of the Office …………

Ans 1. general superintendence and control of the Controller. 2 and conditions of service of Controller, 3. The Head Office and Branch Office 4. of the Controller.

Exercise 3 : True and False

(a) Non exercising supervision over the activities of the Certifying Authorities;

(b) certifying private keys of the Certifying Authorities

(c) laying down the standards to be maintained by the Certifying Authorities;

(d) specifying the qualifications and experience which employees of the Certifying Authorities should possess;

Ans 1. false 2. (False) 3. True 4. True

Exercise 4. Short Question Answers

1. Explain Regulatory Framework Regulation of Certifying Authorities;

…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………

2. Explain Appointment and Functions of Controller;

…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………

3. Define License to issue Digital Signatures Certificate;

…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………
…………………………………………………………………………………………

4. Explain Renewal of License;

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

5. Define Controller’s Powers;

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………