CHAPTER - V

SECURITY ISSUES IN TRADITIONAL CONTRACTS AND ELECTRONIC CONTRACTS
CHAPTER V

SECURITY ISSUES IN ELECTRONIC CONTRACTS

5. Introduction:

Having explored the various intricacies in formation of contract both in traditional form and online contracts along with the jurisdictional aspects in relation to a contract entered through electronic commerce and offline medium, a reference to the security aspects that arise in each has been analysed in this chapter. Commerce depends upon confidence, authenticity, integrity, non-repudiation, writing and signature of the parties. Buyers and sellers must have the same confidence in electronic transaction as they have in traditional kinds of transactions. The issue of authentication and consequently the use of digital signature are vital for two reasons. Parties who wish to engage in e-commerce and enter into an electronic contract will not usually have any means of verifying the other persons’ identity. A person entering into online contracts must be confident of the authenticity of the communication it receives. Integrity is concerned with the accuracy and completion of the communication. Security is often cited as one of the greatest barriers to e-commerce. Indeed, the security system for e-commerce is a business problem not merely a technology problem. This chapter analyses the technological development such as public key encryption that provide critical components of an overall solution. The study in this chapter in the ensuing lines is to see if these forms of security measures are sufficient.

With the internet becoming the sine qua non\(^1\) of everyday life not only business information, but a large amount of personal information too is now digitised and stored on computers connected to the internet. Shopping, payment of various bills, transfer of funds from one account to another, booking of tickets can all be done online. Internet and the electronic contracting have reduced the human labour considerably. Communication and jurisdictional issues which electronic contracts pose has already been dealt with, the electronic transactors are however not very concerned about these two issues. The users

\(^1\) Meaning “indispensable condition”
of the internet are more concerned about the security issues which they project. In electronic contracts the contracting parties never meet each other. All information is exchanged electronically. Every information has its own value of importance and hence needs to be protected. This chapter attempts to focus on the security issues which are associated with electronic contracts.

Systems connected to the internet are potential targets for eavesdropping destruction, tampering of the data stored in them. A website offering services on the internet is vulnerable to attacks, which render the site non-functional resulting in denial-of-service. There may also be instances where masqueraders pretend to be authorised users and gain access to privileged areas. Authorised e-commerce or e-governance transactions could be modified or replaced for commercial gain.

A traditional contract takes place in the real world whereas an electronic contract takes place in the virtual world. In traditional contracts the contracting parties meet each other and discuss the prospects of entering into a valid contract, on the other hand in e-contracts, the parties never see each other face to face. This often raises a sense of suspicion about the identity, the genuineness and the true intent of the other party. Moreover when the contract is with regard to articles, irrespective of the detailed description about the product, the buyer is still at a weaker end for he has no opportunity to personally check the product before he makes a purchase. This buyer has either very little or no opportunity to inspect the product, hence doctrine of caveat emptor would have very little applicability.

A lot of data interchange takes place over the web in e-contracts. As the meeting of minds takes place in the virtual world there is a necessity to ensure data integrity and authentication. While a person is transacting over the internet there must be certainty about the identity of the person and the authenticity of the data interchanged else the very purpose of a contract will be defeated.

5.1 Security aspects with respect to traditional contracts

In the Indian Contract Act 1872, Section 10 emphasises the essential requirements for a valid contract. It states “all agreements are contracts if they are entered into by the free consent of the parties who are competent to contract for a lawful consideration with a
lawful object, are not expressly declared by the act to be void.” Further Section 13 of the Act defines the term ‘consent’ as “two or more persons are said to consent when they agree upon the same thing in the same sense.” Thus, consent involves ‘identity of minds or consensus ad-idem – agreeing upon the same thing in the same sense’. In the absence of this element among the contracting parties there is no real consent and hence no valid contract. Section 14 of the Act defines ‘free consent’ as “consent is said to be free when it is not caused by coercion, undue influence, misrepresentation, fraud, and mistake.” In the absence of free consent the contract may turn out to be either void or voidable depending upon the nature of the flaw in the consent. When consent to an agreement is caused by coercion, undue influence, misrepresentation or fraud there is no free consent and the contract is voidable at the option of the party whose consent was so caused (Section 19 and 19A). But when consent is caused by mistake, agreement becomes void. It is appropriate to quote the words of Lord HANNEN in Huges v. Smith2 “It is essential to the creation of a contract that both parties should agree to the same thing in the same sense. Thus if two persons enter into a contract concerning a particular ship or person, and it turns out that each of them is mislead by a similarity in names, the mistake will be regarding the identity of the person or ship in mind and no contract would come into existence between them:” Raffles v. Wichelhaus3 where the mistake does not defeat the consent, but only misleads the parties, Section 20 should apply. “Where both the parties to an agreement are under a mistake as to a matter of fact essential to the agreement, the agreement is void.” This section will come into operation.

1. When both the parties to an agreement are mistaken,

2. Their mistake is as to a matter of fact and

3. The fact about which they are mistaken is essential to the agreement.

Mistakes are of three types i.e. Common mistake, Unilateral mistake and Bilateral mistake. Identity of the parties – when both the parties to an agreement under a mistake as to the identity and nature of subject matter of the contract – their mistake is as to a

---

2 (1871) LR 6 QB 597,609; 40 LJ QB 221; 25 LT 329
3 (1864) 2 H&C 906: 159 ER 375 33 LJ Ex 160.
matter of fact and the nature and content of the promise itself – fact about which they are mistaken is essential to the agreement. Section 21 emphasises that mistake should be of fact and not law. Only a mistake of fact allows a contract to be avoided. Mistake of fact occurs in two forms unilateral and bilateral (mutual). A unilateral mistake occurs when only one party to the contract makes a mistake as to some material fact important to the subject matter of the contract. The general rule is that a unilateral mistake does not afford the mistaken party any right to relief from the contract although there are some exceptions to this rule. When both the parties are mistaken about the same material fact either party can rescind the contract. Section 22 states about contracts matter of fact. Certain facts are very essential to every agreement they are

1. Identity of the parties
2. Identity and nature of subject matter of the contract and
3. The nature and content of the promise itself.

5.1.1 Mistake as to Identity:-

This occurs where one of the parties represents himself to be some other person. This is what transpired in Jagannath v. The Secretary of State for India\(^4\) “A person called S, a brother of the plaintiff represented himself as plaintiff and thereby induced a government agent to contract with him. The court on finding that the government agent was deceived by the conduct of the plaintiff and his brother held that there was no valid agreement and no contract.” Mistake as to attribute of the party renders the contract voidable and vests a right to rescind with the affected party. Right of recession is however lost if there is lapse of time, acquiescence, third party acquires a right in good faith for consideration before rescission is exercised or if restitutio in integram (restitution) is not possible.

Comparing traditional contract and online contracts, security risks are said to be very minimal for traditional contracts because the parties are meeting in person (in most cases), discussing the terms and conditions and then signing the contract. While on the other hand in online contracts, parties are unaware as to who is on the other end. This is one of

\(^4\) (1886) 21 Punj Rec No. 21, p.37
the main issues that pose a threat for online users. But in a traditional contract too, as far as mistake as to Identity of the parties are concerned there is a lurking danger but however in this field there are time proven set precedents which eliminate uncertainty, relating to the manner in which in these cases justice will be delivered, while in online contracts the issue is not settled.

5.1.2 Fraudulent Impersonation:-

When an innocent party is fraudulently induced to enter into a contract, the contract can usually be avoided because that party has not voluntarily consented to its terms. Under such circumstances the innocent party can either rescind the contract and be restored to his original position or he can enforce the contract and seek damages for any injuries resulting from the fraud. Any form of misrepresentation either by misstatement or omission of a material fact knowingly made with the intention of deceiving another and on which a reasonable person would and does rely to his or her detriment. Fraudulent misrepresentation occurs when one party to a contract misrepresents a material fact to the other party, with the intention of deceiving the other party and the other party justifiably relies on the misrepresentation.5

In Boulton v. Jones6 the plaintiff had taken over the business of one Brocklehurst. The defendant used to deal with Brocklehurst and not knowing of the change sent him an order for certain goods. The order was received by the plaintiff who sent the goods. The defendant came to know of the change only when he received an invoice and by that time he had already consumed the goods. The defendant had a set off against Brocklehurst and therefore refused to pay the price. Four unanimous judges held the defendant not liable. Pollock CB said: “the rule of law is very clear that if you propose to make a contract with A, then B cannot substitute himself for A without your consent and to your disadvantage securing to himself all the benefit of the contract.” “When anyone makes a contract in which the personality, so to speak of the particular party contracted

6 (1857) 27 LJ Ex 117; 157 ER 232
with is important, for any reason, whether because it is to write a book or paint a picture or do any work of personal skill, or whether because there is set off due from that party, no one is at liberty to step in and maintain that he is the party contracted with”.

The principle was further affirmed by House of Lords in *Cundy v. Lindsay*. Here the plaintiff received orders in writing from a fraudulent man called Blenkaran. The order papers had a printed heading: “Blenkaran & Co., 37, Woodstreet.” There was a well known and respectable firm named Blenkiron & Co., in the same street. The plaintiffs believing that the order had come from this firm and sent a large quantity of handkerchiefs. Blenkaran received the goods and disposed them off to the defendants who acted in good faith. The plaintiff sued the defendants. It was held that there was no contract between the plaintiffs and Blenkaran and therefore he had no right to sell the goods. The plaintiff intended to contract with Blenkiron & Co., and consequently no contract could have arisen between them and Blenkaran, “of him they knew nothing, and of him they never thought, with him they never intended to deal. Their minds never for an instant of time rested upon him and as between him and them there was no consensus of minds, which could lead to any agreement or any contract whatsoever.”

There can be a mistake of identity only when a person bearing a particular identity exists within the knowledge of the plaintiff, and the plaintiff intends to deal with him only. If the name assumed by the swindler is fictitious there will be no mistake of identity as held in *King’s Norton Metal C. v. Edrige, Merrett & Co.*. The scope of operative mistake as to identity is further reduced when the parties are in each other’s presence. In *Phillips v. Brooks Ltd.* a man called North entered the plaintiff’s shop and selected pearls and rings worth £ 3000. He produced a cheque book and wrote out a cheque for the amount. While signing he said: “You see who I am, I am Sir George Bullough” and finding on reference to a directory that Sir George Bullough lived at the address mentioned, the plaintiff let him take the ring. He promised to come for the article after the

---

7 Dr. Avatar Singh “Contract and Specific Relief”, Eastern Book Company (15th edn. 2007) p.230
8 (1878) 3 App Cas 459; 38 LT 573; 47 LJ QB 481
9 Ibid 5
10 Court of Appeal (1897) 14 TLR 98.
11 (1919) 2KB 243
cheque was cleared. Before the fraud was discovered he pledged the ring with the defendants who advanced money with a bonafide intention and without notice. The plaintiff sued the defendants for the ring or its value. It was held that the plaintiff intended to contract with the person present before him. Horridge J said: “the mind of the parties met and agreed upon all the terms of the sale, the thing sold, the price and time of payment, the person selling and person buying. The fact that the sellers were induced to sell by the fraud of the buyer made the sale voidable but not void. His intention was to sell to the person present before him and identified by sight and hearing, it does not defeat the sale because the buyer assumed a false name.”

The Court of Appeal in *Ingram v. Little* however again emphasised that even where parties are present face to face mistake as to identity may stand between them and prevent them from reaching the point of true consent. In another subsequent case of *Lewis v. Averay* Court of Appeal pointed out that the title of the innocent buyer from the swindler should not be made dependant on subtleties. In this case Lewis, the plaintiff had a car to sell. A man introduced himself as Richard Green, a famous film actor, tested and like the car and offered a cheque. The plaintiff told him to wait till the cheque was cleared, but when his resistance was broken he demanded proof of identity. The man produced a special pass of admission to a film studio which showed his photograph and official seal. This convinced the plaintiff and he allowed the car to be taken. The man disposed the car to an innocent buyer, the defendant. The worthless cheque came back and the plaintiff sued the defendant to recover his car, Lord Denning said that: “in such cases he should suffer who allowed the possession of his goods to pass without waiting for the cheque to be cleared. When the parties are present face to face the presumption is that the contract is made with the person actually present even though there is a fraudulent impersonation by the buyer representing himself as a different man than he is, where however the identity of the other party is of vital importance to the offeror, a mistake as to identity will prevent an agreement from arising and the importance of identity must depend upon the nature of the promise in each case.”

13 (1961) 1 QB 31; (1960) 3 All ER 332
14 (1971) 3 All ER 907; (1972) 1 QB 109; (1971) 3 WIR 603 CA
nutshell, a mistake as to identity renders the contract void whereas, if the mistake relates to attribute of the person, the contract is only voidable.

5.1.3 Mistake in relation to a written document

There is another class of mistake which is peculiar to the law of written contracts. This is due to the existence of the common law defence of non est factum which permits one who has signed a written document, which is essentially different from that which he intended to sign, to plead that notwithstanding his signature, “it is not his deed” in contemplation of law- “scriptum predictum non est factum sum.” The term applies to deeds but is equally applicable to written contracts also.\(^\text{15}\) The defence of non est factum enables a person who has signed a contract to say that it is not his document; because he signed it by mistake. It was evolved by the courts to relieve illiterate or blind people from the effect of a contract which they could not read and which was not properly explained to them. But subsequently it was extended to others through the judgment in *Foster v. Mackinnon*\(^\text{16}\) where a person was induced to sign on the back of a paper the face of which was not shown to him and he was told that it is an ordinary guarantee and that no liability would fall on him. But in fact the paper was a bill of exchange and he was sued by the holder in due course as an endorser. The court held that the defendant never intended to sign that contract or any such contract. He was actually deceived not merely as to the legal effect, but as to the actual contents of the documents. The defence of non est factum is a narrow one. Those too lazy or too busy to read through the document before signing it cannot rely upon it. DONOVAN L.J explained in *Muskham Finance Ltd v. Howard*\(^\text{17}\) “much confusion and uncertainty would result in the field of contract and elsewhere is men were permitted to try to discard his signature simply by assessing that he did not understand that which he signed. In order for the defence to succeed, the person executing the document must show that the transaction which the document purports to effect is essentially different in substance or in kind form the transaction intended.”\(^\text{18}\)

\(^{15}\) J. Beatson – “*Anson’s Law of Contracts*” Q.C Oxford University Press
\(^{16}\) (1869) LR 4 CP 704; 38 LJ CP 310; 20LT 887
\(^{17}\) (1963) 1 QB 904 at P. 914
\(^{18}\) J. Beatson – “*Anson’s Law of Contracts*”. Q. C Oxford University Press at p.319
In *Saunders v. Anglia Building Society*\(^\text{19}\) an elderly widow gave the title deeds of her house to her nephew intending to make a gift to him of the house in order that he could borrow money on the security of the property. It was a condition of the gift that he was to permit her to reside there for the rest of her life. The nephew came to her with one Lee and Lee told her to sign a document saying that it was a deed of gift to the nephew and that everything was in order. As she had broken her spectacles she could not read the contents but put her signature witnessed by her nephew. The document was an assignment in favour of Lee. He mortgaged the house with the building society and having defaulted in payment the society claimed possession. She pleaded non est factum. House of Lords held that she was bound by the contract and that it was only voidable by reason of the misstatements made by Lee, but it was too late to avoid once the building society had advanced a sum of money on the house in good faith.

She was not, therefore mistaken about the character of the document. The only thing was that it was put to a use which she did not expect. Lord DENNING pointed out that the plea of non est factum is a plea which must necessarily be kept within narrow limits. Lord WILBERFORCE emphasised that the law in respect must retain flexibility because it has to reconcile two conflicting objectives, relief to a signer whose consent is genuinely lacking and protection to innocent third parties who have acted on an apparently regularly and properly executed document.\(^\text{20}\)

The Supreme Court of India considered the principle in *Ningawa v. Byrappa Hirekarabab*\(^\text{21}\) where a husband obtained the signature of his wife to a gift deed without making any representation as to its character, but subsequently included two or more plots in the deed, the transaction was only voidable and not void. Where a person signs a document in blank leaving it to another to fill in the terms of the contract in accordance with an oral agreement reached between them, it would seem that he could in theory rely on the defence of non est factum, if the terms inserted render the transaction essentially different in substance or in kind from the transaction intended. However unless there are exceptional

---

\(^{19}\) (1971) A.C 1004
\(^{20}\) Dr. Avatar Singh “*Contract and Specific Relief Act*”, Eastern Book Company, (10\(^{th}\) edn.) p.251
\(^{21}\) AIR 1968 SC 956 (1969)2 SCR 797
circumstances present, a person who signs a document in blank accepts responsibility for it and he takes the risks even if through fraud or error, the document is filled in the same way. He cannot therefore avoid his liability as against an innocent third party.\textsuperscript{22}

Thus we see in traditional form of contracts also where parties meet in person and enter into contracts there are certain risks involved. But there are clear provisions in the Contract Act and precedent English Law cases which are still binding on the Indian laws. Thus solution for the problem is already there. Being forearmed is being forewarned.

5.2 Security aspects with respect to Online Contracts:

The three major concerns for international electronic contracting are authenticity, enforceability and confidentiality. Authenticity involves the verification of the person that one is dealing with electronically. Enforceability includes the legal scope of the license granted or the warranty given under a national law. It also includes the provability and verification of the contractual terms of an online transaction. Confidentiality revolves around the protection of sensitive information such as payment information and trade secrets. The fear is that the public domain nature of e-commerce makes such information, susceptible to fraud and misappropriation by third parties. The minimum level of due diligence pertaining to these three concerns entails a workable knowledge of the legal requirements of forming and proving a contract formed through the internet. The most secured means of internet contracting is the entering into a trading partner agreement with a known party.\textsuperscript{23} The techniques that can be used to authenticate the existence of the other party and to confirm the terms of the contractual undertaking include acknowledgment, use of independent agents or value added networks and encryption. Acknowledgment can be an email or facsimile that confirms the online transaction.\textsuperscript{24}

5.2.1 Various kinds of Security Threats

Security is often considered as one of the greatest barriers to e-commerce. Computers can also be programmed for other nefarious activities submitting hundreds of

\textsuperscript{22} J.Beatson QC, “Anson’s Law of Contract” Oxford University Press (27\textsuperscript{th} edn. 1998) p.322
\textsuperscript{23} Gary S Weinstein, “Forming Contracts on the Internet, Corporate Counselling Quarterly” 14 (1998);
\textsuperscript{24} Larry A. Dimatter “Law of International Contracting” Wolter Kluwer (2\textsuperscript{nd} edn. 2009)
fraudulent orders or probing for ways to gain access to a computer system. On an insecure computer system an attack may leave no trace. Crimes in the physical world always leave evidence like footprints, fingerprints, pictures on security camera and so on. The following are the various kinds of security threats posted by the cyber space:

a) Cyber Attacks:

Attacks can be classified as executable-based or network based. In the case of the former, the attack happens only when a program is executed on the targeted computer system through either of the following:

- **Trojan** - a computer program that appears to have a useful function, but also has hidden and potentially malicious functions that evade security mechanisms, sometimes by exploiting legitimate authorisations of a system entity that invokes the program. The idea of modifying a normal program to do nasty things in addition to its usual function and arranging for victim to use the modified version is known as a Trojan horse attack.²⁵ It was the Trojan house attack which in earlier times in traditional setting created the proverb ‘Beware of Greeks bearing gifts.’

- **Virus** - a program fragment that is attached to a legitimate program with the intention of infecting other programs. It is hidden, self replicating computer software, usually malicious logic, that propagates by infecting, i.e., inserting a copy of itself into and becoming part of another program. A virus cannot run by itself; it requires its host program to be run to make the virus active.²⁶

- **Worm** - a computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. It differs from a virus only in that a virus piggybacks on an existing program, whereas a worm is a complete program itself. Viruses and worms both attempt to spread themselves and both can do severe damage. The Conficker worm is a computer worm that can infect a

²⁵ www.exploria.com (Last accessed on July 17, 2013)
²⁶ www.ecybercrime.com (Last accessed on July 17, 2013)
computer and spread itself to other computers across a network automatically, without human interaction.²⁷

- **Spam** - is also a major source of cyber attacks. There are some estimates according to which 70% of all e-mail is junk mail or spam. While spam by itself has nuisance value in that it clogs most of the internet highways around the world causing losses by way of improper utilisation of bandwidth, it is used to propagate viruses and worms. Junk mail appears to be promotional material, similar to advertisements and catalogues in the physical world. Unsuspecting users become victims as soon as they click on attachments. Trojans and spy-ware get installed on their systems.

- **Denial-of-service attacks** - A Denial-of-Service or DoS attack is an attack on a network that is designed to disable the network by flooding it with useless traffic or activity. A distributed denial-of-service attack uses multiple computers to launch a DoS attack. A DoS attack does not do any technical damage, but it can do substantial financial damage to an e-business. These attacks are extremely difficult to defend against. In a traditional denial-of-service attack, the victim’s computer might be able to figure out where the attack is coming from and shut down those connections. In a distributed attack, there is no single source. The computer should shut down all connections except the ones it knows to be trustworthy. In order to protect systems from executable – based attacks, anti-virus measures must be deployed on desktops, servers and on the corporate gateway for data coming in from external sources.

**b) Hacking:**

Externally accessible systems are targets of hacking. Hackers can deface websites and steal valuable data from systems resulting in a significant loss of revenue if it is a financial institution or an e-commerce site. In the case of corporate and government systems, loss of important data may actually result in the launch of information espionage or information warfare. Using IP Spoofing, attackers often hide of machines used to carry

²⁷ [www.microsoft.com](http://www.microsoft.com) (Last accessed on July 17, 2013)
out an attack by falsifying the source address of the network communication. This makes it more difficult to identify the sources of attack traffic and sometimes shifts attention onto innocent third parties. From the study conducted by this researcher it is ascertained that nearly 72 percent (71.4 percent) of the corporate respondent have never faced problems of hacking while nearly 23 percent of them have faced it for 1 to 5 times.\textsuperscript{28} It can be applauded that the corporate sector is taking adequate measures to counteract Hacking. Though in the course of survey, the corporate were reluctant to disclose their security measures, it is highly appreciable to know that major portion of respondent have not been hacked.

c) Weak Authentication:

Security handling teams estimate that many incidents stem from the use of weak, static passwords. Passwords on the internet can be cracked in a number of different ways. However, the two most common methods are by cracking the encrypted form of the password and by monitoring communication channels for password packets. The UNIX operating system usually stores an encrypted form of passwords in a file that can be read by normal users. The password file can be obtained by simply copying it. It can also be obtained by a number of other intruder methods. Once the file is on hand, an intruder can run readily available password cracking programs against the passwords. If the passwords are weak, e.g. less than 8 characters, and so on, they could be cracked and used to gain access into the system.

d) Ease of Spying:

It is important to note that when a user connects to his account on a remote host using Telnet or FTP (File Transfer Protocol), the user’s password travels across the internet unencrypted or in plaintext. Thus, another method for breaking into systems is to monitor connections for IP packets bearing a username and a password, and then using them on the system for normal login. If the captured password is to an administrator’s account, then the job of obtaining privileged access is made much easier. Hundreds and possibly thousands of systems across the internet have been penetrated as a result of

\textsuperscript{28} Chapter VI, table 6.4.15 Frequency of the company websites being hacked p.260.
monitoring for usernames and passwords. E-mail, as well as the contents of Telnet and FTP sessions, can be monitored and used to obtain information about a site and its business transactions. Most users do not encrypt e-mail, since they assume that e-mail is secure and thus safe for transmitting sensitive information.

e) **Phishing:**

It is the creation of e-mail messages referencing web pages that are replicas of existing sites to make users believe that these are replicas of existing sites to make users believe that these are authentic sites. Unsuspecting users are made to submit personal, financial, or password data to such sites from where the data get directed to fraudsters chosen sites. The findings of this research study reveals that with respect to the problems faced because of Phishing or Hacking by the banker respondents, expose that 66.7 percent of the respondents have ‘Never faced’ problems of phising or hacking while 28 percent have ‘Rarely faced’ the problem and a very trifling 5 percent has stated that they face problem very often.\(^\text{29}\) Thus it can be concluded that when two-third of the banker respondents have never faced problems of phising or hacking indicates strong security measures maintained by the banker

f) **Spoofing:**

The IP address of a host is presumed to be valid and is therefore trusted by TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) services. A problem is that, using IP source routing, an attacker’s host can masquerade as a trusted host or a client. In other words IP spoofing is used by intruders to gain unauthorised access to computers. Messages are sent to the computer with the sender IP address of a trusted system. Packet headers of the message are modified to make it appear that the message is coming from a trusted system.

E-mails can easily be spoofed and hence without enhancements such as digital signatures, they cannot be trusted. For example, consider the exchange that takes place when internet hosts exchange mail. The exchange takes place using a simple protocol consisting of ASCII (American Standard Code of Information Interchange) character

\(^{29}\) Chapter VI, table 6.3.7 Security Measures taken by the Banker to Prevent Phishing and Hacking, p.236.
commands. An intruder could easily enter these commands on Telnet to connect directly to a system’s SMTP (Simple Mail Transfer Protocol) port. The receiving host trusts this sending host, and thus the origin of the mail is spoofed easily by entering a sender address that is different from the true address. As a result, any user, without privileges, can falsify or spoof e-mail.\(^{30}\) The research amazingly discloses that among the banker respondents when compared to the awareness about Salami attack and Data diddling, spoofed e-mail is quite higher as little more than 50 percent (51.3 percent) have stated “Yes, very well” and followed by that nearly 39 percent (38.5 percent) have stated “I have heard about it, not sure.”\(^{31}\) The banker respondent plays a vital role in equipping themselves about the cyber threat and communicates the same to the customer. The study reveals that nearly 28.2 percent have stated that they educate their customers about cyber threats, while 62 percent of the banker respondents have not responded.\(^{32}\) The researcher opines that the banker respondents have bounden duty to impart technical knowledge about online banking and various cyber threats. 93.8 percent of the customers have not revealed their awareness about e-mail spoofing.\(^{33}\)

**g) Credit Card Fraud and Theft of Customer Data:**

Almost all B2C purchase transactions involve credit cards. An e-business that accepts credit cards in payment for goods and services, must secure the credit card information in transit to its website, and it must secure stored credit card information. Also, systems must be in place for credit card transaction authentication and credit card authorisation.

A hacker can break into a database server and steal thousands of credit card numbers and other information in a matter of moments and an e-business might not even recognise that the hacker was there. For example, one of the largest reported cases of stolen credit card information in January 1999 (but was not reported until much later) when information on 4,85,000 credit cards, including card numbers, expiration dates, names and addresses was stolen from an e-business website was stored at a US government agency’s website, where

\(^{30}\) Spoofed e-mails appear to originate from one source but actually it has been sent from another source. www.codefh.blogspot.com (Last accessed on July 17, 2013)

\(^{31}\) Chapter VI, table 6.3.4 Awareness of spoofed e-mails p.230.

\(^{32}\) Chapter VI, table 6.3.5 Customers educated about Cyber threats p.234.

\(^{33}\) Chapter VI, table 6.5.11 Awareness of email spoofing p.275.
the agency’s website administrator discovered the data. There was no reported evidence of fraudulent use, and some of the accounts were not active. But this event highlights the risk to a vulnerable e-business of the theft of sensitive information.

h) Web defacement:

Web defacement is the substitution of the original home page of a website with another page by a hacker. Religious and government sites are regularly targeted by hackers in order to display political or religious beliefs. Disturbing images and offensive phrases might be displayed in the process, as well as signature of sorts to show who was responsible for the defacement. Websites represent the image of a company or organisation and these are therefore especially vulnerable to defacement. Visitors may lose faith in sites that cannot promise security and will become wary of performing online transactions. After defacement websites have to be sometimes shut down for repairs causing expenses and loss of profit. The highly commendable part of the research is to know that the almost ¾ (74.2 percent) of the Government Department respondents have stated that their departments have never been a prey for web defacement or web jacking. Nearly 20 percent (19.4 percent) stated that attempt was made but it was duly prevented by security measures. The study has also brought to light that the departments have taken proper security measures to counteract the threats. Nearly 13 percent (12.9 percent) have stated that they use secure passwords and frequent changing of password. Another 13 percent (12.9 percent) have stated that they have installed fire wall and antivirus. But the most astonishing part is nearly 62 percent (61.3 percent), the major portion the respondents have not disclosed the security measures, taken by them to counteract these threats. Nearly 63 percent (62.9 percent) of company respondents failed to disclose whether they faced web defacement or web jacking. Only 17 percent (17.1 percent) have stated that they have faced and a little more than that 20 percent have stated they have never faced problems of web defacement. The corporate entities should take adequate measures for counteracting this kind of offence.

35 Chapter VI, table 6.2.5- Website of the Government Department has ever been preys for Web Defacement or Web jacking and security measures taken by the Department to counteract these threats. p.215.
36 Chapter VI, table 6.4.14 Awareness of Web defacement or web jacking p.259.
i) Data Diddling:

One of the most common forms of computer crime is data diddling – illegal or unauthorised data alteration. These changes can occur before and during data input or before output. Data diddling cases affect banks, payrolls, inventory records, credit records, school transcripts and virtually all other forms of data processing known. The study reflects that only a negligible 6.5 percent of the government staff are “very well aware” about Data diddling while nearly 55 percent (54.8 percent) have responded that “they have heard” about this and 38.7 percent “do not know” about it. Hence it can be evidently understood that the Government department staff must be educated intensively about the various cyber threats and the devastating consequences of the same.

From the research it is perceived that nearly 28.2 percent of the banker respondents are “very well aware” about the Data diddling, while nearly 49 percent (49.7 percent) “have heard about it but not sure” and 23 percent (23.1 percent) “do not know” about it. It is not sufficient if the banker respondent have heard about it; they should be aware and have sound knowledge about it. It is sin qua non for every banker to equip themselves with the latest technological development and take sufficient measures to curb the cyber threats. They cannot exempt themselves by taking the plea of non-awareness. Further 80 percent of the corporate customers have not revealed whether they are aware about Data diddling or Salami attack. It is highly alarming to know that a major portion of respondents are not willing to disclose, this can be either due to confidential reasons or may be due to sheer lack of knowledge. The researcher is of the opinion that the corporate should be mandated to follow certain rules and regulation framed by the government with respect to Electronic transactions. This systematic study conducted with respect to banker respondent about the serious threats in electronic transactions brings to light that as far as the Indian sector is concerned. ‘Data diddling’ is considered as the most serious threats followed by spoofing and salami attacks. Hence the banker should equip with sound security measures to counteract these cyber crimes effectively.
j) Salami Attacks:

These attacks are used for committing financial crimes. The key here is to make alteration so insignificant that in a single case it would go completely unnoticed. For instance, a bank employee inserts a program, into a bank’s server, that deducts a small amount of money (say Rs. 2 a month) from the account of every customer. No account holder will probably notice this unauthorised debit, but the bank employee will make a sizeable amount of money every month. The researcher has deciphered from the study conducted that nearly 58 percent (58.1 percent) of the government respondent who offer electronic mode of payment have heard about salami attack, but they are not sure about it. A little more than 40 percent (41.9 percent) are not aware about this grave cyber crime which goes to show the lack of awareness among the government department employees.\textsuperscript{40} To overcome this, the government should impart proper training and educate them about the consequences of salami attack.

With respect to the Banking respondents nearly 26 percent (25.6 percent) have very well knowledge about salami attack, while 48.7 percent have heard about it but are not sure. The most astonishing part is 25.6 percent of the bankers are ignorant about salami threat.\textsuperscript{41} This has grave consequences if the banker is left unaware of the issue. They should be forewarned about this threat. The researcher was astonished to know that 80 percent of the corporate respondents have not answered whether they are aware about ‘Salami attack’.\textsuperscript{42} This reveals the ignorance of the corporate and it is high time that they impart sound training to their employees. Ignorance of cyber threats will prove to be very fatal to the corporate sector.

k) Key loggers:

They are used to log all the strokes a victim makes on the keyboard. This assumes sinister proportions, if a key-logger is installed on a computer which is regularly used for online banking and other financial transactions. Key-loggers are most commonly found in public computers such as those in cyber cafes, hotels etc., and unsuspecting victims also end up downloading spyware when they click on friendly offers for free software.

\textsuperscript{40} Chapter VI, table 6.2.3 Awareness of Salami attacks p.212.
\textsuperscript{41} Chapter VI, table 6.3.2 Aware of salami attacks p.230.
\textsuperscript{42} Chapter VI, table 6.4.12 Awareness about data diddling or Salami attack p.257.
From the study conducted it shows that only 48.7 percent of the banker respondents “have heard about key loggers, but are not sure about it”, while 28.2 percent are “very well aware” about it and 23.1 percent have accepted that “they don’t know” about key loggers. This is a serious threat for customers who access their account from unknown places. Hence the banker owes responsibility to their customers in educating them about this cyber threat and the consequences of the same. This research further reveals that nearly 80 percent (79.5 percent) of the banker respondents have not disclosed about the precautionary measures taken by the bankers to educate their customer while accessing their bank account at cyber cafe. Only 15.4 percent have given a positive reply that they “educate their customers”, while a very negligible 5 percent (5.1 percent) have stated that they “do not explain” the precautionary methods while accessing their account in cyber cafe.

The banker while providing variety of banking and other services must ensure that the customers have a sound knowledge of cyber threats and the various implications of the same. 50 percent of the customer respondents are “not aware” about key loggers while 32.5 percent “know” what it is. Though only 17.5 percent of the respondents are “very well aware” about key loggers, 44.47.5 percent of them “knew about virtual keyboard”.

l) Web Jacking:

Just as the conventional hijacking of an airplane is done using force, similarly web jacking means forcefully taking over control of a website. The motive is usually the same as hijacking – ransom. The perpetrators have either monetary or political purpose which they try to satisfy by holding the owners of the website to ransom. This occurs when someone forcefully takes control of a website by cracking the password and later changing it. The actual owner of the website does not have control over what appears on the website.

m) Cyber Terrorism:

Terrorism refers to the use of force and violence to intimidate or subjugate, especially as a political party. Terrorists intimidate or coerce a government or its people

---

43 Chapter VI, table 6.3.6 Awareness of Key loggers and Precautionary measures taken by the banker to educate their customer while accessing their account at cyber cafe p.235.
44 Chapter VI, table 6.5.7 Awareness of key loggers p.271.
45 Chapter VI, table 6.5.8 Awareness of the virtual keyboard p.272.
by instilling fear among them. Terrorist threats include damage and sabotage of property, personnel and facilities with the intention of spreading fear. It is the use of internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses. It is a controversial term. Some authors choose a very narrow definition, relating to deployments, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic. By this narrow definition, it is difficult to identify any instances of cyber terrorism. Cyber terrorism can be also defined as the intentional use of computer, networks and public internet to cause destruction and harm for personal objectives. Objectives may be political or ideological since this is a form of terrorism.

There is much concern from government and media sources about potential damages that could be caused by cyber terrorism, and this has prompted official responses from government agencies. Cyber terrorism 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.

5.3 Measures to Combat Security Threats:

Having had an overview of the different kinds of cyber issues arising in the cyber space, there is a necessity to study the methods to counteract these acts. Internet has its advantages and disadvantages. As the advantages outweigh the disadvantages we cannot do away with internet and cyber transactions. There are various security systems to counteract these issues. The solutions to the above problems are discussed briefly hereunder.

5.3.1 Firewall

An internet firewall is a system or group of systems which aid in enforcing a security policy between an organization’s network and the internet. The firewall determines which inside services may be accessed from outside, which outsiders are permitted access to the permitted inside services and which outside services may be accessed by insiders. A firewall

46 Matusitz, Jonathan – “Cyber terrorism: American Foreign Policy interests” (April 2005)
must be able to restrict unauthorised access and must be immune to penetration. If an attacker succeeds in getting through or around the firewall it can no longer offer protection. A firewall system can be a router, a personal computer, a host or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnet. The firewall is part of an overall security policy. A firewall improves network security and reduces risks to hosts on the subnet by filtering insecure services. A firewall could prohibit certain vulnerable services such as Network File System (NFS) from entering or leaving a protected subnet. This provides the benefit of preventing the services from being exploited by outside attackers, but at the same time permits the use of these services with greatly reduced risk exploitation.

5.3.2 Anti-virus Softwares

Antivirus softwares are used to prevent, detect and remove malware (of all descriptions), such as computer viruses, Keyloggers, Trojan Horses, Worms etc., Computer security, including protection from social engineering techniques, is commonly offered in products and services of antivirus software companies. A variety of strategies are typically employed. Signature-based detection involves searching for known patterns of data within executable code. However, it is possible for a computer to be infected with new malware for which no signature is known. For such type of malware, generic signatures can be used to identify new viruses or variants of existing viruses by looking for known malicious code, or slight variations of such code, in files. Some antivirus software can also predict what a file will do by running it in a sandbox and analyzing what it does to see if it performs any malicious actions. Despite the advantages and uses, antivirus software can have drawbacks. Antivirus software can impair the performance of a computer. The users must be experienced enough to understand the prompts and decisions of the antivirus software for, an incorrect decision may lead to a security breach. Hence user education plays a vital role. If the antivirus software employs heuristic detection, success depends on achieving the right balance between false positives and false negatives. False positives can be as destructive as false negatives.

---

5.4 Execution of contracts in cyberspace:

The traditional contract is executed on a paper and duly signed by the parties to the contract. The ink and paper concept has become obsolete because of the invasion of current Information Technology. In the 2nd chapter how formation of a contract is being analysed. The elements of offer, acceptance, intention to create legal obligations are required be it an online or offline contract. Only the mode of execution differs. Traditional offline world has over a period of time developed very many settled legal principles that govern the actions and rights of the parties. The cyber space is comparatively a fairly recent invention and jurisprudence in cyber law is still at a nascent stage which is gradually developing while certain laws applicable to the conventional offline can be adapted successfully to the online contracts also but not all traditional legal principles will find its application or fix into the complex realm of cyberspace.

Traditional laws may be adapted or new laws may need to be framed as transacting through paper and through cyberspace is totally a different scenario. In the traditional form a valid contract is recognised through the authenticity and genuineness of the parties who affix their signatures which help in identifying the parties and further that they are accepting to the terms and both duly sign the agreement in ink and paper. In cyberspace how the identity of the parties fixing of signatures are done are two main issues. There is a general consensus that electronic signatures and electronic documents are legally valid and stand on equal footing to the ‘ink and paper’ signatures. What a seal and signature is to a paper document, digital signature is to an electronic document authenticity of the document and identification of its maker is what digital signature aims at. Signature is a thing of the paper world; it is a stamp of authenticity and a traditional way of saying that a document is both original and approved by the writer. The queer world of cyberspace knows no copy and everything is original there.50 The UNCITRAL working group on electronic commission framed the model Law on Electronic Commerce in 1996.51 The model law presents a set of internationally acceptable rules that assist in resolving legal complexities

50 Tatalat Fatima, Dr. “Cyber crimes” Eastern Book company, Lucknow (1st edn. 2011) p.27
in electronic commerce and aims to create a secure environment on the internet. The model law emphasises on the principles of “Fundamental Equivalence.” According to this approach the functions of a traditional paper based document and a handwritten signature can be well achieved using electronic documents or electronic signatures respectively. In the year 2000 India enacted its first law of Information Technology based on these fundamental principles elucidated in the Model Law. There are certain legal issues which confront us on the internet relating to the authenticity and identity of the parties integrity and competency of the parties: These are discussed in this chapter.

5.5 Identity of the parties in an electronic contract

The sender of an internet communication cannot necessarily be presumed to be who he says he is nor can the sender be always sure of the recipients’ true identity, say for instance, A sends an email from his email id – A@yahoo.com the presumption is ‘A’ has sent this mail to ‘B’. ‘B’ believes that the contents of the mail have come from the mail id of ‘A’ which means it is from ‘A’. There are possibilities that ‘X’ or ‘Y’ can use A’s mail id and sent mail, they might be sending this either on directions given by ‘A’ or without his knowledge by fraudulent means like hacking the password and sending it through ‘A’s mail id. The recipient of the mail ‘B’ is not aware if it is ‘X’, ‘Y’ or whether it is under ‘A’s directions or is it without ‘A’s knowledge that an email has been sent to him. In the same way in the recipient end ‘A’ cannot always be sure that it is being read only by ‘B’ it could be hacked and somebody else might read on reply. Here again two possibilities are there, person replying from ‘B’s email id should be doing either with his knowledge or under his direction or the other way is without his knowledge by unlawful means. Furthermore email message being like an open post card can be intercepted at any place on line, modified, altered, changed and made to appear to have come from a person other than the actual sender and the worst part of it is that the recipient cannot detect it. Similarly a business can set up its own website over which goods or services can be offered without revealing true identity. There are instances where business can setup a website in one country but made to appear to have premises in another country. Recently in Australia a scam was unearthed in which “internic.com” a website was launched with a name similar to the official domain name registry, Inter NIC whose current site is at “internic net.” Before this fraud is detected, it is believed that over 13,000 people
throughout the world were defrauded. While creating an electronic mail id, few may give their actual names, while some may give the initials whereby people dealing with them can identify them by the id. There are people who choose anonymous mail id to hide their identity completely. Other types of Internet communication also lack clear identification of the communicating parties. In some cases this uncertainty as to identity raises no problems i.e., when the identity of the email address itself is not going to identify the person. If the dealings are going to be contractual with flow of consideration and legal consequences then it is very important to know about the identity of the address’s owner. If the disclosure of the identity of the contracting parties over the internet is not possible, then many of the fundamental principles of the common law for contract formation will be either inapplicable or simply irrelevant. Whether in a physical environment where parties are at a distance or in cyberspace, before executing a contract, the contracting parties must be sure about (i) party sending or receiving the communication as the case may be (ii) communication (iii) time of communication. For instance A and B communicate an offer and acceptance for executing a contract over internet ‘B’ must be assured that the (a) offer received is the one sent by A, (b) offer received by him is the same sent to him, meaning there should not be any alteration or it should not be corrupted in transit, (c) time of dispatch of offer, (d) offer received is meant for him. In the same manner ‘A’ must have the same surety when he receives acceptance from ‘B’. One method of identifying a party is to use the identity information provided by the person. This might be included in an email perhaps as part of the email ‘signup’ option.

If a user is viewing a website, a form can be used which requires the user to input identification details. But here again the authenticity, credibility of the identification arises. This method can be adopted on the basis of a trust or good faith. This cannot be the proper form of identification because if the communication between the parties is going to be legally binding transactions like formation of a contract the recipient may need to enforce the terms of contract subsequently, hence this sort of identification would be inadequate. Proper identification is essential even of the recipient, because they may

52 Dr. Farooq Ahamed – “Cyber Law in India (Law on Internet)”, New Era Law Publication, Delhi. (2nd edn. 2005) p.245
go for some other legal obligation or financial dealings. One method of overcoming this problem can be to check the identity of the user with the internet host identified in the communication. But here again there is a difficulty, because the host may be unwilling or unable to release that identity in formation, this might be because the host or the user may be in a jurisdiction where data protection laws apply or in other cases the host may have adopted a privacy policy which prevents the disclosure of personal information. Say suppose the host is willing and is also permitted to disclose the information the quality of that information will be unknown to the recipient. In general there is no obligation on the hosts to take formal identification of their subscribers where host charges for internet access are probable that credit card details would have been taken and checked. However where ISP’s provide free internet access, paid for via a revenue sharing agreement under which the ISP and the users telecom provider share the connecting telephone call charges, as such no such identity check is normally made.53 In an offline transaction this problem is often overcome by requiring the parties to produce residence proof, identity proof issued the government usually a passport copy, driving license, ration card, PAN card, voter’s id card are taken into consideration. The challenge for the internet is to develop analogous identification tokens which are effective for digital transactions. This has been achieved by establishing specialised third parties whose function is to take identification evidence and issue electronic identification tokens. But here again there are number of legal issues. The infrastructure and technological advancements used to identify internet user have been developed as part of the search for an effective method of signing electronic documents. As far as security aspects are concerned it is analysed as two separate issues one pertaining to the identification of the parties and the other is validity of the signature. The technology which produces many risks for the parties entering into online contract has also provided solution for all the issues and it is for the parties to adopt any of the available technologies.54 However in the Indian scenario IT Act provides no alternative for the parties except to adopt asymmetrical cryptosystem and hash functions.

At present, the identity of the transacting party is verified with password, electronic signatures and Internet Protocol addresses. However, a more effective system of digital certification and authentication needs to be developed for which efforts is being made around the globe. From the research, it is revealed that nearly (42.9 percent) of the corporate respondents have “never” faced problems relating to identity of a customer or supplier, while 51.4 percent faced it “rarely”.  

5.6 Issues relating to Electronic Mistake

One among the most cumbersome issues discussed in legal literature with respect to electronic contracting is treatment of mistake. Since the electronic communication takes place often between pre-programmed devices, very rapidly and at a distance, mistakes might be difficult to notice and correct. On 25th Nov 2005 the United Nations General Assembly adopted a new convention on the use of Electronic Communications in International contracts. This convention on e-contracting is the most important and long awaited development in International electronic commerce law. This new convention aims to enhance the legal certainty and commercial predictability of International contracts where electronic forms of communication are used. Being mainly concerned with the formation of electronic contracts, it recognises the value of electronic communications and modernizes the terminology of older conventions to embrace the impact of digital technologies. The aim of the convention is to remove legal obstacles to electronic commerce including those which arose under other instruments on the basis of the principles of functional equivalence – which is the most fundamental principles of electronic commerce law. The convention sets the criteria to be used for establishing functional equivalence between electronic communications and paper documents as well as between electronic and handwritten signatures. It aims to provide a common solution in a manner acceptable to states with different legal, social and economic systems. This treaty expressly recognises a contract formed by a computer system and a natural

55 Chapter VI, table 6.4.7 Problems relating to identity of a customer or supplier p.253.
57 ibid
person or by the interaction of automated message systems. Such contract shall not be

denied validity or enforceability on the sole ground that no natural person reviewed or

to each of the individual actions carried out by the automated message

systems or the resulting contract. In consequence, automated transactions of Internet

merchants are treated as paper based deals of traditional entrepreneurs. The treaty

regulates consequences of a contractual mistake in the following article “Article 14,

where a person makes an input error on an interactive website and is not given the

opportunity to correct it he or she has the right to withdraw the portion of the electronic

communication if he / she:-

a) notifies the other party of the error as soon as possible and

b) has not used or received any material benefit or value from the goods or services

if any received from the other party.”

The treatment of electronic mistake is ‘expressis verbis’ meaning expressly

limited to transactions concluded via interactive websites and not through passive

websites, emails, chat or EDI. Only the person who made an input error has the right to

withdraw from it. This has to be promptly notified to the other party. For exercising this

right of withdrawal the person should have received any benefit out of the transaction –

e.g. downloading software from the website and then trying to return the same and finally

the uncertainty in this is non specification of time limit for the exercise of the right of

withdrawal thereby introducing complexity in the system. But critics argued that such

provision might conflict with well established contract law principles and it is more

appropriate for consumer transactions and that it would create serious difficulties for trial

courts, since the only evidence of the error would be the assertion of the interested party

that she has made an error.58

The proponents argued that the type of error is specific to electronic communication

and deserves special treatment, that it provides a much needed uniform rule in view of the

differing and possibly conflicting national rules and that it did not in any way aggravate

the evidentiary difficulties that already exist in a paper based environment; because court

58 Ibid
would have to assess all the circumstances anyway. The purpose of this provision requires clarity. The drafters felt that such a prescriptive provision would be incompatible with the “enabling nature” of the convention.

5.6.1 Importance of Signature in traditional contracts

In the traditional form of contract a contract is given its validity on the basis of the authenticity and genuineness, a signature is appended or inked by the parties to identify the parties and originality of unhampred terms agreed by them akin to an original written and duly signed agreement in ink and paper. The oral agreements are valid and enforceable in certain jurisdictions, but are difficult to prove with evidence in a court of law. Paper based contracts are duly signed by the contracting parties and this is universally accepted as it is easier to prove in court of law. The written signatures carry a particular function i.e., to bind the parties to the terms and conditions specified in the contract and ensures non-repudiation. The paper based signatures authenticates the person who is signing the document and also it is an authentication of the document also whereby the person is refrained from changing the signed matter without tampering. There is a clear indication of parties that they intend to be bound by the terms contained in a document. A signature is the manifestation of the will to sign “the animus signandi” – meaning the intention of being recognised as the signer who has agreed to be bound by the document that he so finds. The ceremonial function of signing means there are legal implications of the act and further there is clarity and finality to a transaction.

Safety can never be an absolute state compared to the level of fraud affecting other forms of consumer purchasing, at times internet appears to be safe. When a person hands over his credit card to the person across the shop counter or when he gives it to a waiter in a restaurant or when he reads the number over the telephone to make a purchase is taking a far greater risk that the card might be fraudulently used than a consumer on a secure internet connection. Apart from it exchange of written documents would consume more time, energy and cost. Now that paperless transactions are most welcome, they are eco-friendly and nowadays most of the bills, phone bills and card statements are sent online.
5.6.2 Importance of signature in online contracts

Security is a property of the whole system. For instance a security of a bank depends on its vaults, guards, video cameras, motion sensors, vigilance of employees etc., In the same manner security of an electronic commerce system requires appropriate technology, but it also requires a clear understanding of what is being protected along with careful operation and monitoring the people running it. In the present study conducted it is highly commendable to know about the customer feeling of securities upon the bankers. Study reflected that 25.6 percent of the customers felt the banker was ‘very secure’ while a little more than 60 percent (61.5 percent) felt it was ‘secure’ to transact with their bank.

An electronic contract is an agreement created and signed in an electronic form – where no paper or other hard copies are used. For instance say ‘A’ emails an offer to a business associate ‘B’ and ‘B’ gives acceptance by mail with an electronic signature affixed to the mail offer, it can be concluded that a valid and binding contract has been formed between A and B. An e-contract can also be in the form of a ‘Click to Agree’ contract, commonly used with download software. The user clicks an ‘I agree’ button on a page containing the terms of the software license before the transaction can be completed. Since a traditional ink signature is not possible on an electronic contract, people use different ways to indicate their electronic signatures including typing the person’s name into the signatures area or else pasting a scanned version of the signers signature clicking an ‘I accept’ button or using cryptographic scrambling technology. At the same time there may be some uncertainty in using online authentication, particularly problems of unauthorised interception, identity thefts, cheating by personating and anonymity in cyberspace. It is also easy to tamper electronic document without easy detection. To combat with these challenges use of sophisticated techno legal solutions to fulfil the functional equivalent approach i.e. equating – e-signed documents with paper signed documents has therefore gained material importance. The most prevalent

60 Chapter VI, table 6.3.12 Customers Response about the Security offered by the Banker p.244.
e-signature technology is the asymmetric cryptosystem which creates a digital signature using two different asymmetric cryptographic keys.

Digital signature has become the most commonly used and accepted method. It functions for electronic documents like a handwritten signature does for printed documents. The signature is an enforceable piece of data that asserts that a named person wrote or otherwise agreed to the document to which his signature is attached.

A digital signature actually provides a greater degree of security than a handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been altered either intentionally or accidentally since it was signed. Secured digital signatures cannot be repudiated; the signer of a document cannot later disown it by claiming the signature was forged. Digital signatures enable ‘authentication’ of digital message, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.62

Electronic commerce activity has now largely been facilitated by use of electronic signatures in online transactions. It has become a very common practice to use digital signatures to sign and file documents to incorporate a company in India with the Registrar of companies. Even in government office in some places in India, a digital signature, digipad is used for authentication and identification. All these developments have brought about a shift in the legal approach to the concept of privacy. With the emergence of e-commerce a host of personal information like credit card numbers, details of various electronic transactions, medical and insurance etc are being transferred through the internet. Personal resumes and other personal information are also available on the net. Data kept in personal computers which are hooked to the net, have become accessible. Therefore organisations on the internet, including corporate bodies, governments, universities, banks and other institutions are apprehensive that hacker or unauthorised persons may enter into the systems and engage fraudulent transactions, manipulate records or sabotage the computerised data. Hacking of electronic records has become a hobby for many amateur hackers. While the internet and the

62 www.legalservicesindia.com (Last accessed on November 13, 2013)
Global Information infrastructure continues to grow in terms of quality and quantity. E-commerce has been emerging as the principal medium of commercial prosperity. This has kindled the interest of individuals and corporate alike in cryptography. It is an art of secret writing – keeping information secret. When applied in computing environment cryptography can protect data against unauthorised disclosure; it can authenticate the identity of a user or programmer requesting service and it can disclose unauthorised tampering. Encryption of information to prevent it being read by unauthorised person is a major component of the data security system.

This method was extensively used by the government intelligence agencies in order to protect military secrets and confidential matters. Later this method has become popular with corporate bodies, for protection of confidential data. The results of the study conducted revealed that 48.6 percent (48 percent) of the company respondents are “very well aware” about it, while 28.6 percent are “not sure” about digital signatures. It is also understood that almost a little more than one – fourth of the corporate respondents possess digital signature, while 31.4 percent stated they “intend to procure” digital signature in the future. Nearly 43 percent of them “do not possess” a digital signature.\textsuperscript{63}

5.7 The Technical Aspects of Encryption

Encrypting emails, files and even entire data storage prevents unauthorised people from accessing them. Encryption provides protection against breaches of confidentiality for both company and personal data. Cryptography comprises encryption, i.e., the process of making information unintelligible to the unauthorised reader, and decryption, i.e., reversing encryption to make the information intelligible once again. Conventional cryptography uses a secret code or key to encrypt information. The same secret key is used to decrypt information.

5.7.1 Cryptography – Based Solutions

Cryptographic systems or cryptosystems are symmetric or asymmetric. The symmetric system is based on single secret key which is shared by the parties engaging in secure

\textsuperscript{63} Chapter VI, table 6.4.8 & 6.4.9 Awareness of digital signatures & Possession of digital signature. p.254
communication. The asymmetric system hinges on the possession by these parties of a pair of keys – one private and other public.

Modern encryption is achieved with algorithms that use keys to encrypt and decrypt messages by turning text or other data into digital code and then by restoring it to its original form. The length of the key determines the code's security level. The longer the key, the more secure the code. To decipher an encrypted message without access to a key, a person would need to try every possible key. Computer keys are made of bits of information, binary units of information that can have the value of 0 or 1. Therefore, an 8-bit long key has 256 \( (2^8) \) possible values. A 56-bit key creates 72 quadrillion \( (72,000,000,000,000,000,000) \) possible combinations. Without the key to crack a 56-bit encrypted message, a person would have to resort to the so-called brute-force method to decrypt the message i.e., try out every single one of the 72 quadrillion possible combinations. If the key is 128 bits long, attempting to crack the code without the key would be 4.7 sextillion \( (4,700,000,000,000,000,000,000) \) times more difficult than cracking a 56-bit key (which itself has 72 quadrillion possible combinations). Given the current power of computers, experts consider that a 56-bit key could be cracked by using the brute-force method in 10 million hours of computer time (14,000 computers used around the clock for 4 months). Cryptography can only hide information after it is encrypted and while it remains encrypted. But information generally does not start out encrypted so there is normally an original period during which the secret is not protected. Such information generally is not used in encrypted form, so it is again outside the cryptographic envelope every time the information is used. It can hide words but not physical contraband, cash, physical meetings and training, movement to and from a location, an extravagant lifestyle with no visible means of support or actions. In the same way cryptography cannot protect against informants, under-cover- spying, bugs, photographic evidence or testimony. The problems with physical key is we tend to lose our keys, forget which key is for what, might give to neighbour, friends or might go to the hands of a wrong person, somebody can steal the key, can pick the lock or break open

---

64 Professor Lawrence Lessig – “Code and Other Laws of Cyberspace”. Basic Books. 1999 used in mobile communications, and the latter is used for encryption / authentication.
the lock, can go through the window or break open the door or burn the house or legally enter into the house on a warrant, so on and so forth. Hence it is seen absolute perfect keys also cannot solve all problems nor can they guarantee privacy. Indeed when cryptography is used communications generally at least two people know what is being communicated, so either party could reveal a secret either by accident to someone else, through third party eavesdropping or as revenge for actions real or imagined or for payment or under undue influence or in testimony. When it is substantially less costly to acquire the secret by means other than a technical attack on the cipher cryptography has pretty succeeded in doing what it can do.

5.7.2 Symmetric Cryptography

This is historically known as the Secret Key System. In this crypto system, the same key is used to encrypt and decrypt the information. There are two types of symmetric key crypto systems: ‘stream’ ciphers and ‘block’ ciphers, the former is Symmetric systems are built by repeatedly using mathematical operation involving the key. Thus, they can be executed at a high speed. In the symmetric system, the secret key is shared between two persons or entities; hence it is very important to make sure that the mode of exchange of the secret key is secure. It has greater chances of being compromised and for this reasons asymmetric cryptography is preferred to symmetric cryptography.

5.7.3 Asymmetric Cryptography

While symmetric cryptography uses a single secret key to encrypt and decrypt a message, asymmetric cryptography uses two keys – a public key which is known to everyone and a private key which is known only to the owner. This is one of the most important and widely accepted methods of signing electronic documents technically known as Public Key Cryptography or Public Key Infrastructure (PKI) model. The digital signature affected by use of PKI method is one of the forms of affixing electronic signature. Using the public key anyone can encrypt a message, but only the other corresponding key in the key pair will be able to decrypt it. Although these keys are related to one another, it is practically infeasible to find out the private key using the public key. A signer signs with his private key and a recipient decrypts the message with the public key which assures reliability and verifies sources of origin of a message.
On encryption, hash value matches with decrypted message hash value which will remain the same if the message has reached the recipient unhampered. This hash function when applied to a message of any length creates a short fixed value which is known as message digest or hash value. It is unique to the message and the given private key. The hash function produces the same hash value each time when applied to the same message. Hence it is also called one way process because it is computationally infeasible to reconstruct the same message from its hash value. The changes of two messages producing the same hash value are insignificantly small. If there is a slight change in the message contents, entirely different hash result will be produced. Once the hash result of the message is computed by the signer’s software it is then transformed into what is known as digital signature by the signer’s private key. Say for example ‘A’ is interested in making an offer to ‘B,’ A instead of encrypting the whole message, will apply the hash function to produce a hash result. The hash result will be transformed into what is technically known as a Digital Signature by the private key of A. Then he will send that offer to B along with its digital signature. B will apply the same hash function to the offer to get its hash value. Then using the public key of A the hash value thus produced, B will verify

i. Whether the digital signature was created using the corresponding private key.

ii. Whether the hash value produced by him matches with the hash value sent to him by A which was transformed into the digital signature.

This technology ensures integrity of the message but does not prevent impersonation. For an example say ‘B’ does not know ‘A’. Applying this technology even with a hash function will not enable B to know A. Anyone can generate a key pair by impersonating another. In order to prevent this issue, there must be a trusted third party who will independently confirm the identity of the parties, their location and legal

---

67 Digial Signature Guidelines – American Bar Association (Information Security Committee)
status. In this technology verification of a digital signature means checking as to whether the digital signature was created for a particular message and signed by the private key that relates to the public key associated with it.

5.7.3.1 Steps involved in digitally signing a message:

During the digital signature process, the following steps are undertaken by the signer or recipient of the digitally signed message.

Step 1: The signer is the owner of a unique PKI key pair.

Step 2: The signer writes a data message on his computer or takes an already written message.

Step 3: The signer uses a secure hash algorithm to create a ‘message digest’. A hash result is formed which is unique to the signed data message.

Step 4: The signer further encrypts the message digest by signing with private key. The digital signature comprises of the encrypted data message digest.

Step 5: The signer attaches his digital signature to the message to be transmitted.

Step 6: The signer sends the digitally signed message to the recipient through computer.

Step 7: The recipient uses the signer’s public key for verifying the signer’s digital signature. The fact that the message was sent by the signer is also verified by use of public key.

Step 8: The recipient creates a message digest of the message using the same hash algorithm.

Step 9: The recipient then compares the two message digests which should be the same if the message is not altered.

Step 10: The recipient procures a certificate form Certification Service Provider to confirm the digital signature of the signer. This certificate usually contains public key and full name of the signer, verified by the Certification Service Provider.


70 Whittle, Robin “Public Key Authentication Framework; tutorial”1996; http://www.beinrohr.sk/sxool/ing_semester1/kubiki (Last accessed on November 09, 2013)

This system is based on a one way mathematical function – easy in one direction but very difficult to reverse, as for example, multiplying two very large numbers is easy but factorizing this product can be very difficult. Diffie – Helman, RSA, El Gamal are based on this theory. Asymmetric key crypto systems are flexible to implement as compared to secret key systems, but are much slower to execute. This system is widely used in digital signature, key management and entity authentication.

In order to achieve both confidentiality and authenticity, the message can first be authenticated using the originators private key and the authenticated message can then be made confidential by encrypting with the recipient’s public key. Since the secret key does not have to be shared between communicating entities in public key cryptosystems, the chances of the secret key being compromised is reduced. Although theoretically, the public key can be used to determine the corresponding private key, its infeasibility (within time and cost constraints) is built over the difficulty of solving certain mathematical problems. Apart from PKI electronic signatures can be affixed using other methods of verification such as use of biometrical device involving handwritten signatures where a signer signs manually using a unique pen like device on a digital pad or directly on a computer screen. This signature would be converted and stored in an electronic form in a computer and attach to a data message for authentication. Other biometrics based on electronic signatures include retina scanning, iris patterns, finger printing that records an individual’s specific print or quality and measurement as identity proof and authentication. Further personal identification number (PIN) such as internet password or I-pin or password authentication or clicking the ‘OK’ or ‘I agree’ button to enter into e-contract with the name typed at the end of the message just like a click wrap agreement where one’s identity can be determined through IP address or prior registration in a site or even a sound on click of a button on cell phone to give consent are other modes of electronic signatures. The reliability is judged based on the security mechanism used. For eg: in digital signatures security mechanism used is asymmetric cryptography.

---


5.7.4 RSA Algorithm

One of the most popular and widely used public key cryptosystems is the RSA algorithm, developed in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology (MIT). Few other examples of public key cryptosystems are Elgamal (named after its inventor Taher Elgamal), Diffie-Hellman (named after its inventor) and DSA, Digital Signature Algorithm (invented by David Kravitz)

5.8 Application of encryption in E – Contracts

The success or failure of e-contracts depends upon various factors, including the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have taken place on popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations. Every e-commerce entrepreneur is highly concerned about the security of the information which is stored or communicated, for the loss of data can be detrimental to both profitability and future business prospects. Asymmetric cryptosystem is no doubt an effective way to combat cracking an unauthorised access to confidential information. On one had people are trying to create unbreakable codes while on the other there is another set of people trying to break through the codes to attain unlawful gain.

In order to enable secure online transaction, data encryption plays four important functions:

- Digital authentication allows both the customers and the merchant to be sure that they are dealing with whom the other party claims to be. This is absolutely necessary before sending credit card details to the merchant and also allows merchants to verify that the customer is the real owner of the credit card being used.

- Integrity ensures that the messages received are not changed during transmission by any third party.

---

• Non-repudiation prevents customers or merchants denying they ever received or sent a particular message or order.

• In the event that information is intercepted, encryption ensures privacy that prevents third parties from reading and or using the information to their own advantage.

5.9 Advantages of Encryption to E-Contracts

Encryption is used in many ways on the web today. The following are the benefits of encryption in e-contracts:

   **Financial Data of the Consumer** – Protection of credit card and banking information of the consumer when they are purchasing items online is one of the most common uses of encryption on the web. The encryption allows the information to be safely transferred and used by the retailer for the purchase transaction. The same kind of software that encrypts the information during input is used to decipher it on the receiving end.

   **Email privacy** – Encryption is used to keep email messages private. Individuals needing their information to be secure, such as missionaries working in dangerous areas, and government entities, use email encryption regularly.

   **Online Banking** – No one would use online banking if they felt they were risking access to their bank accounts by outsiders. Online banking sites use very strong encryption software.

   **PayPal transactions** – PayPal has become one of the most used and trusted sources for transferring funds on the internet. To keep its users protected, Paypal keeps its data encrypted.

   **Online accounting** – Several accounting programs for small businesses now offer online accounting options. Well maintained encryption is a key ingredient in keeping the business information safe and secure from hackers.

   **Online backup services** – If one uses an online backup service, the information he backs up to their servers is being encrypted to keep it safe from theft and viewing by unauthorized users.
Virtual Private Networks (VPN’s) - It relates to the ability to privately access a small network from a remote location. In order to allow only authorized users into the network, powerful encryption and security tools are used.

File sharing/transfers – Transfer of computer files has become quite common. Encryption is part of the process that keeps your data safe as it is being moved from server to another.

Remote logins – There are services on the internet that allow you to remotely login to your home or work computer from another location. These remote login services must be protected from intruders with encryption software.

Government Security – Governments are the other big users of encryption on the internet. Keeping their information and communications secure from capture is a matter of national security; hence they take this very seriously.

5.10 Concept of Digital Signatures

Digital signatures are used not only to verify the authenticity of the message and the claimed identity of the sender, but also to verify message integrity. The technology has assumed huge importance recently, with the realisation that it may be the remedy to one of the major barriers to growth of electronic commerce: fear of lack of security. Digital signatures provide data integrity, thereby allowing the data to remain in the same state in which it was transmitted in addition to authenticating the identity of the sender to third parties.

The digital signatures offer certain advantages as against their traditional handwritten counterparts. The digital signatures provide the proof of data integrity by giving an assurance that the data has not been altered either accidentally or intentionally. It also provides authentication which involves identifying the sender of the message. The authenticity of a traditional signature must be established through a notary public, on the other hand in the digital world, certificate authorities provide the necessary authentication. A digital signature provides evidence in the event of the signer and recipient of a document denying the existence or integrity of the transaction thus ensuring that the message is not repudiated by either party. Digital documents can be signed and
transmitted around the world in just a matter of few seconds and can be processed faster and more accurately through automated systems. Thus the possibility of errors, delays and misrouting are reduced with the advent of digital signatures. The date time stamp plays a vital role in the implementation of a digital certificate for the date and time will be used to verify the validity of certificates. A digital signature ensures that only individuals who have access to the key to decrypt the message will be able to access the contents of the message, thus ensuring confidentiality. A digital signature provides security as the data used for computing the digital signature partially originates from the information itself making it possible to establish a link between the authentication and the information provider. It depends on the text to be encrypted therefore it can never be identical to every message. As a result any third person cannot forge or tamper with a digital signature.

Using, the RSA algorithm, a message is encrypted with the sender’s private key to generate the ‘signature.’ The message is then sent to the destination along with his signature. The recipient decrypts the signature using the sender’s public key, and if the result matches with the copy of the message received, the recipient can be sure that the message was sent by the claimed originator and that the message has not been modified during transmission, since only the originator is in possession of the corresponding encryption key.

5.11 Secure Electronic and Digital Signature

The term electronic signature is used to describe the full range of electronic means to confirm the sender of the message. They range from a file including graphical image of the sender’s handwritten signature which is simple but unreliable to biometrics techniques such as iris scan though complex it is reliable. Electronic signature may be defined as any symbol or method adopted by a party in the process of validation provided there is an existing intention to be bound by or to authenticate a record accomplished by electronic means. Though not all electronic signatures perform the key functions of a handwritten signature viz., authentication, non – repudiation and data integrity these can

---

be achieved by a subset of electronic signature i.e., Digital Signatures. However other electronic signatures provide security by merely providing passwords.

A secure digital signature must satisfy the following conditions:

1. It should be unique to the subscriber affixing it. A digital signature is unique to and is based upon the message that is signed and the private key of the signer.

2. It should be capable of identifying such subscriber. What this implies is that the digital signature should be verifiable by the public key of the signer and by no other public key.

3. It should be created in a manner or using a means under the exclusive control of the subscriber. This implies that the signer must use hardware and software that are completely free of any unauthorised external control.

4. It should be linked to the electronic record to which it relates in such a manner that if the electronic record were altered, the digital signature would be invalidated. All standard software programs used to create digital signatures contain this feature. Without this feature, the whole purpose of creating digital signature would be defeated.\(^7\)

5.12 Legal Purposes of Digital Signatures

The processes of creating a digital signature and verifying it, accomplish the essential effects desired of a signature for many legal purposes:

5.12.1 Signer Authentication:

If a public key and a private key pair are associated with an identified signer, the digital signature attributes the message to the signer. The digital signature cannot be forged, unless the signer loses control of the private key, such as divulging it or losing the media or device in which it is contained.

5.12.2 Message Authentication:

The digital signature also identifies the signed message, typically with far greater certainty and precision than paper signatures. Verification reveals any tampering, since

\(^7\) Section 15 of the Information Technology Act, 2000
the comparison of the hash results (one made at signing and the other made at verifying) shows whether the message is the same as when signed.

5.12.3 Affirmative Act:

Creating a digital signature requires the signer to use the signer’s private key. This act can perform the ceremonial function of altering the signer to the fact that the signer is consummating a transaction with legal consequences.

5.12.4 Assurance:

The processes of creating and verifying a digital signature provide a high level of assurance that the digital signature is genuinely the signer’s. As with the case of modern Electronic Data Interchange (EDI), the creation and verification processes are capable of complete automation (sometimes referred to as machinable), with human interaction required only in exceptional cases. Compared to paper methods such as checking specimen signature cards – methods so tedious and laborious that they are rarely used in practice – digital signatures yield a high degree of assurance without adding greatly to the resources required for processing.

The processes used for digital signatures have undergone thorough technological peer review for over a decade. Digital signatures have been accepted in several national banks, government agencies. The likelihood of a malfunction or a security problem in a digital signature cryptosystem designed and implemented as prescribed by the industry standards is extremely remote and is far less than the risk of undetected forgery or alteration on paper or of using other less secure electronic signature techniques.

5.13 Secure E-Payment Process

Secured payment transactions play a vital role in e-commerce. Electronic contracts are built on the cornerstone of secure e-payment systems. If the contracting parties have a sense of insecurity during the payment process the very purpose of an e-contract would be defeated. It is thus essential to have a secure mode of payment, failing which the parties to the contract are likely to lose confidence in electronic transactions. There are two common standards for secure e-payments – SSL and SET. Both these security measures use public key cryptography for encryption and authentication.
5.13.1 SSL (Secure Socket Layer)

SSL is a secured socket layer between HTTP and TCP on a web server. It is a transport layer security protocol. SSL provides a simple encrypted connection between the client’s computer and merchant’s server over the internet. It also provides authentication for the merchant’s server with its digital certificate from a certificate authority. This is a secured connection for cyber shoppers to send payment information to e-seller’s web shop. The SSL encrypts and decrypts information flowing between the two computers. In other words it encrypts both HTTP requests and HTTP responses. The SSL provides a secure connection than that of the traditional postal mail delivery. The security however ends at the merchant’s site. The most important boon of the SSL is that it does not keep the credit card numbers of the transaction is completed.

5.13.2 SET (Secure Electronic Transactions)

SET is a messaging protocol designed by VISA and MasterCard to enable secured transactions over open networks, such as the Internet. An SET protocol has three players – the customer, the merchant and the merchant’s bank. The following are the three principal features of an SET protocol.

- All sensitive information sent within the three parties is encrypted.
- All three parties are required to authenticate themselves with certificates from SET certificate authority.
- The merchant never sees the customer’s card number in plain text.

The third feature actually makes e-contracting more secure than that of the traditional credit card transactions, such as pay by credit card in store or through mail order form. It is more secure as compared to the SSL. To implement SET in e-commerce on internet, it requires the SET point-of-sale client software such as SET “electronic wallet” implemented widely in the client’s web browser. It is a big challenge to make such point-to-sale software widely available to the internet community.
5.13.3 Trusted Third Parties (TTP)

In cryptography, a trusted third party (TTP) is an entity which facilitates interactions between two parties who both trust the third party; The Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content. In TTP models, the relying parties use this trust to secure their own interactions. TTPs are common in any number of commercial transactions and in cryptographic digital transactions as well as cryptographic protocols. For example, a certificate authority (CA) would issue a digital identity certificate to one of the two parties. The CA then becomes the Trusted-Third-Party to that certificate’s issuance. Likewise transactions that need a third party recordation would also need a third-party repository service of some kind or another. Trusted Third Parties perform the function which a witness performs in a traditional contract.

5.14 Merits and Demerits of the Available Security System

The firewall system which prevents unauthorised penetration aids in stopping unauthorised users from accessing our system. However if the firewall system is weak it can easily be breached. So it is important to ensure that the firewall system of the system is up to date and strong enough to prevent penetrations. Even if the firewall system is strong enough, if the unauthorised person manages to break into the firewall or go around it, it can be of no further use. Hence a better system may be developed whereby even if a penetration occurs, there are sufficient means to curb the malware from harming our secured information.

5.14.1 Level of Security in Government Department

In this research the researcher has to highly appreciate the government department respondents where, 32.3 percent have stated that they communicate with their customers ‘Very often’ about the level of security offered by them, while 38.7 percent of them do it ‘rarely’, while 26 percent (25.8 percent) never communicate with their customer’s.77 The researcher is of the opinion that the Government departments must be mandated to

77 Chapter VI, table 6.2.6 Level of security offered by the Government department website to the customers. p.216.
inform their customers about the various security measures taken by them. It is further understood from the study that 64.5 percent of the Government department have revealed that their software provider is Trustworthy, while 25.8 percent of them have revealed that their software provider is ‘Very trustworthy’. The Government should enact rules directing all the departments, to purchase their software only from very trustworthy software providers. By implementing the same the security measures can be strengthened and the various cyber crimes can be prevented. From the research conducted it is understood that in the Indian Scenario, the bankers have taken security measure to prevent Phishing or Hacking. Various measures include educating the customers, warning them about the threats, awareness programmes being conducted regularly secured and frequent changing of passwords, identifying banking images and codes and preventing the customers from using unknown links of unsecured websites. The research study conducted brings to light that the bankers are taking enough precautionary methods to be adopted regarding cyber offences to their customer in frequency levels of once in a month, or once in 6 months or once in a year.

Antivirus software’s prevent the malware, viruses, Trojan horses, worms etc., from harming our system. However new variants of existing malware and new malware are being created and are being spread via internet. Hence just antivirus software is insufficient; there is a necessity to update the software periodically to protect our information. The users must be educated adequately about the intensity of harm the malware is capable of causing to their computers. Further when the antivirus software deducts a virus and suggests action or asks for a decision, it is important that the user takes the right decision or acts in the right manner, failing which the very purpose of the antivirus software will be defeated.

Data encryption is an effective way to ensure that our information is secure and free from threats of being tampered with. Symmetric encryption uses the same key to encrypt and decrypt the information hence the parties need seek a trustable source for the communication of the key. Presuming the existence of such a mode of communication. It could be said that there is no necessity to encrypt data. Asymmetric cryptography has abolished the need for a safe and trusted mode of communication of the key.

78 Chapter VI, table 6.2.7 Trustworthiness of the software provider p.217
The existence of a public key which is known to all and a private key which is known only to one self has solved the said problem. Despite the existence of a sound system to ensure data integrity and authentication, not many are aware of a digital signature and moreover the procedure to obtain a digital signature is a lengthy one. Hence people must be educated about the existence and working of a digital signature. The procedures to obtain a digital signature are quite discouraging so though a person is aware of the existence of encryption, he might prefer not to have a digital signature. The mode of online payments is secured using SSL or SET. SET is more secure as compared to SSL, thus a secure mode of payment can be ensured. Just like the tedious procedure behind obtaining a digital signature exists, the implementation of SET in e-commerce requires the SET point-of-sale client software such as SET “electronic wallet” to be implemented widely in the client’s web browser. It is a very challenging task to make such point-to-sale software widely available to the internet community. A much easier method of implementation has to be deduced in order to encourage the usage of a more secure system. The implementation procedures should not be a hurdle in using a much beneficial system of security.

5.15 Legislative Landscape with Respect to Electronic Signatures in the International Arena

The guidelines laid down by various international organisations on electronic signatures are discussed in the following lines. They are nonbinding and have a persuasive value on any nation. India has adopted a technologically neutral approach to electronic signatures as propagated by UNCITRAL Model Law on Electronic Signatures, 2001.

5.15.1 UNCITRAL Model Law on Electronic Signature 2001

The United Nations’ Commission on International Trade Law (UNCITRAL) working group of Electronic Commerce framed the Model Law on Electronic Commerce in 1996. The UNCITRAL Model Law on Electronic Signatures was drafted and

approved in the year 2001.\textsuperscript{80} Many countries including Thailand, India and Mexico have based their legislations governing Electronic Signatures and Electronic Commerce on the UNCITRAL. The Model Law of Electronic Signatures adopts a technologically neutral approach and does not approve or specify any particular form of electronic signature for authentication purposes. The Model Law also explains the rules of conduct to indicate the obligations of the signer, the recipient and the role of a Trusted Third Party, meaning the certifying Authorities that grant electronic signature to a person.\textsuperscript{81} Article 2(1) of the Model Law of Electronic Signatures defines an electronic signature as data in electronic form affixed to a data message and describes his consent to the content in such data message.

The model law envisages three functions of electronic signatures namely, creation and reliance on an electronic signature and certification by a Certifying Authority. More than three entities could be involved when an electronic signature is affixed. Sometimes two of its functions could be fulfilled by a single party in case where the relying party also plays the role of a certifying authority.\textsuperscript{82} United States’ basic contractual rules are found in the Uniformed Commercial Code and State judicial opinions published by the Restatement of Contracts. It applies to the electronic contracts for the sale of goods.

\textbf{5.15.2 Uniform Electronic Transactions Act (UETA)}

The Uniform Electronic Transactions Act (UETA) is another important US legislation applicable to electronic contracts enacted in 1999. UETA uniformed rules were proposed by the National Conference Commissioners on Uniform State Laws (NCCUSL) in 1999. 46 states of United States, the District of Columbia and the U.S Virgin Islands have incorporated UETA rules within their State rules. UETA, as expressly defined in Articles 3 and 4, only applies to transaction related to business, commercial and government matters and to transactions conducted by electronic means. The UETA defines an e-signature as an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent

\footnotesize{\textsuperscript{80} United Nations UNCITRAL Model Law on Electronic Signatures 2001 www.uncitral.org/2001_signatures.html (Last accessed on September 11, 2013) \\
\textsuperscript{81} “Model law on Electronic Signatures with Guide to enactment 2001”, www.uncitral.org (Last accessed on November 14, 2013) \\
\textsuperscript{82} Section 15 of the Information Technology Act, 2000}
to sign the record. A record is information that is inscribed on a tangible medium or that is stored in electronic or other medium and is retrievable in perceivable form. This definition of e-signatures includes encrypted digital signatures, names which are signed towards the end of the e-mail and click on a web page if the click includes the identification of the person. The UETA also states among other things, that a signature may not be denied legal effect or enforceability solely because it is in electronic form. In 2000, congress enacted the Electronic Signatures in Global and National Commerce Act (E-Sign Act) to provide that no contract record or signature may be denied legal effect solely because it is in the electronic form. Electronic signature is as valid as a signature on paper and an electronic document can be as enforceable as a paper one. For an electronic signature to be enforceable, the contracting parties must have agreed to use electronic signatures. For an electronic document to be valid it must be in a form that can be retained and accurately reproduced.

The Electronic Signature Act expressly excludes its application to the following namely wills, codicils or testamentary trusts, family law matters like adoptions, divorce, court orders, official court documents evictions, foreclosures, health insurance terminations and pre nuptial agreement. The only agreements governed by the Uniform Commercial Code that falls under this law are those covered by Articles 2 and 2A and UCC 1-107 and 1-206. Despite its limitations Electronic Signature Act expands enormously the possibilities for contracting online. The Uniform Computer Information Transaction Act (UCITA) is a relevant set of rules covering contracts involving computer information. It means information in electronic from detained from or through use of a computer or that is in digital or equivalent form capable of being processed by a computer.

83 UETA 102(8)
84 UETA 102(15)
85 Roger Le Roy Miller (Institute of University Studies Arlington, Texas) Gaylord A. Jentz (Herbert D Kelleher Emeritus Professor in Business Law – University of Texas at Austion) – “Law for E-Commerce” West Legal Studies in Business
86 UCITA 102(10)
5.15.3 Role of Certifying Authority in Public Key Infrastructure Model (PKI) with reference to UNCITRAL Model Law of Electronic Signatures

The role of a Certification Authority is very crucial in the PKI system and the certifying authorities are authorised to issue digital signatures to its applicants. On the internet different entities or individual interact and transact business who may not have personally communicated with each other before through other means of communication. The verification as to whether an electronic signature belongs to a particular signer can be determined through records of the Certifying Authorities by using the Public Key of the person which contains information such as the complete name and address of the person. The third party i.e., Certification Authority assists in verifying the identity of the signer. The PKI system therefore assures the transacting parties that the messages sent are form the original signer and remain unhampered during the transmission and the cryptographic mechanisms are fairly secure as a private key remains confidential with the signer.

Often the PKI system renders a broad spectrum of services, including management of cryptographic keys, testifying that a particular public key corresponds with a unique private key, providing the private keys to the subscribers, maintaining a repository of public keys and certificates of digital signatures managing smart cards that stores individual private key, time stamping service amongst services. According to the UNCITRAL model law on Electronic Signatures 2001 each country may in its own discretion adopt a PKI model based on technical, legal and public issues. Therefore, discretion is wide enough to cover issues such as number of hierarchical levels of authority that should be formed in a PKI, the power to issue the cryptographic keys should or not lie with public entities, private entities, private entities whether a licensing or other methods may be used to control and supervise the certification authorities.

---

whether a key escrow will apply or not. There is an existing debate over recognition of foreign certification authority as each country has its own certification authorities. The UNCITRAL Model Law on Electronic Signatures 2001 recommends that the maximum cross certification should be adopted so that there is ‘mutual recognition’ and interoperability between PKI structures. However cross certification may have its own set of pitfalls as different countries are free to adopt the PKI model they consider appropriate and different countries may have different security policies and in case of lapses on part of the authorities the enforcement of penalties may lead to a dispute with regards to appropriate forum and application of law of a given jurisdiction. Indian Information Technology Act 2000 Section 19 confers recognition to Foreign Certifying Authorities. The section emphasises that the controller with prior approval of the Central Government has the power to recognise any Foreign Certifying Authority as a Certifying Authority. On receiving such recognition the electronic signature certificate issued by such Certifying Authority shall be valid for the purpose of the Information Technology Act 2000. The powers to revoke such recognition vests with the controller who may revoke the recognition in case the Foreign Certifying Authority contravene any condition or any restriction under which it was granted recognition. The Certifying Authority digitally signs the certificate it issues to the end user. Therefore it is termed as a digital signature. It can be verified by using the public key of the certifying authority mentioned in another certificate issued by a different certification service provider. There is another method in which such verification is possible. Sometimes a digital signature of the issuing authority is recorded in a certificate issued by the certification service provider, generally known as Root Certificate. The certification service provider needs to adopt many security practices independent working, audits by independent entity and enough financial resources for its functioning, key escrow, facility, safeguards and controls to protect its own private key, record its suspension and termination measures and revocation of licenses amongst other

It is important to comply with the prescribed standards laid for issuing the digital signature and the credibility checks to verify the identity of its applicants.

In many countries, the role of a Trusted Third Party (TTP) or certification service provider is compared with a Notary Public. A cyber notary, or legally recognised Certification Authority, issues the key pair identifies the owner of the keys and certifies the validity of the public key. The cyber notary also serves as a repository for public keys. Cyber notaries are available but they do not operate within any existing legal framework because they are so new. There are problems pertaining to equipments and software arising from the inconsistency of technical standards and interoperability. It also envisages plethora of legal hurdles relating to electronic authentication and signature methods and recognises the need to harmonize technical standards as well as laws. Here it is recommended that the legislators should appreciate the need for uniformity in adopting common forms and procedures to recognise electronic signatures both at domestic level and internationally in order to recognise electronic signatures issued by foreign certifying authorities and avail reciprocal benefits in foreign jurisdictions.

As electronic commerce is an international concept, successful functioning, reliability and authenticity plays a vital role hence in order to successfully adopt electronic regime for cyberspace, harmonisation and in laws, technical interoperability issues, recognition and adoption of cross certification practices constitute prime factors for consideration by every nation’s legislators and policy makers.

The Digital Signature Guidelines by the American Bar Association (ABA) are in the nature of a soft code that prescribe a legal frame work wherein adequate security mechanisms are put in place to verify the identity of a subscriber of a private key. It aims to provide a framework that allows effective use of Digital Signatures for e-commerce

---


94 UNCITRAL – document promoting confidence in Electronic Commerce – Legal issues on International use of electronic authentication & signature methods
transactions.\footnote{American Bar Association (ABA) Digital Signature Guidelines http://www.abanet.org/scitech} It provides legal recognition to electronic signatures by making them admissible on legal proceedings. The guidelines envisage the risk allocation and responsibility principles. The electronically signed messages are verifiable to check the authenticity of source and the message transmitted. It legally binds the signer to the private key.\footnote{Ibid 71}

The American Bar Association (ABA) has developed a Model Electronic Data Interchange Trading Partner Agreement that can be tailored to particular types of transaction.

The International Chamber of Commerce (ICC) in 1997 published a guide titled ‘General Usage for International Digitally Ensured Commerce’ (GUIDEC) which addresses some of the definitions and legal aspects relating to methods aimed at overcoming e-commerce authentication and confidentiality problems. It provides a general frame work for ensuring and certifying of digital messages. GUIDEC is national law neutral and its goal is to harmonize legal and trade practices across national legal systems.\footnote{GUIDEC ‘A Living Document,’ accessed at www.iccwbo.org/guidecz.html (Last accessed on} The GUIDEC describes how risks and liability allocation may be made between the parties to a transaction aligned with existing business practices. It gives details of the rights and obligations of subscribers, certifying authorities and the recipient party. GUIDEC aims to promote e-commerce through secure e-transactions and establishes core legal principles that lead to dependable certification practices. It aims to prevent digital frauds and technical errors during electronic transmission and spread awareness on the benefits of using electronic signatures.\footnote{Karnika Seth “Computers, Internet and New Technology Laws” Lexis Nexis Butterworths Wadhwa Nagpur (1st edn. 2012)}

The GUIDEC also refers to the digital signature guidelines drafted by the American Bar Association and explains some of the concepts contained therein form a Lex Mercatoria perspective. The GUIDEC also refers to the UNICITRAL Model Law on Electronic Commerce and relies on the role of digital signatures in the Model Law of Electronic Commerce.\footnote{International Chamber of Commerce, ‘GUIDEC’ www.iccwbo.org (Last accessed on May 18, 2013)} In a digital system, a third party certifies issues a certificate

\footnote{International Chamber of Commerce, ‘GUIDEC’ www.iccwbo.org (Last accessed on May 18, 2013)}
guaranteeing the identity of the sender of an electronic message.\textsuperscript{100} The liability of the certifying company is likely to be contractual in nature. GUIDEIC provides that the certificate should indicate its scope both in duration and transactional longevity. It should state a time period of coverage and whether it certifies a single transaction or a number of transactions. The certificate should also possess a certification practice statement that describes the practices utilised by the certifier in issuing the certificate.

The certifying company will likely place a disclaimer on its certification. A certifier may seek to restrict liability for the contents of a relationship with the subscriber or by means of a general disclaimer in the practice statement, or even in the certificate itself. The prudent trader should examine those instruments for such disclaimers. These disclaimers may not be enforceable under a given national law. National laws should also be reviewed to determine any required formalities relating to warranty disclaimers.\textsuperscript{101}

5.16 Regulatory Framework with respect to Electronic Signatures – in the Indian Scenario

Technological development has converted paper transactions into paperless transactions. Information Technology has established new standards of speed, efficiency and accuracy in communication which eventually have become a source for innovations, creativity and increasing overall productivity. In order to keep pace with the changing scheme, the Indian Parliament passed the much awaited Information Technology (IT) Act, 2000. It draws its inspiration from the Model Law on Electronic Law (UNCITRAL). It received the presidential assent on June 19, 2000 and was implemented as the Information Technology Act, 2000. The Act contains 13 chapters, 93 sections and 4 schedules. Main aim of the act is providing legal recognition to electronic commerce transactions and facilitating electronic filing of documents with Government Authorities. The Information Technology Act, 2000 grants legal validity and recognition to digital signatures and electronic records which is recognised through section 10A.

\begin{flushright}
\textsuperscript{100} Michael Froomkin, \textit{“The Essential Role of Trusted Third Parties in Electronic Commerce,”} Oregon Law Rev, p.75
\end{flushright}

\begin{flushright}
\textsuperscript{101} Larry A. Dimatter – \textit{“Law of International Contracting”} Wolter.S. Kluwer (2\textsuperscript{nd} edn. 2009)
\end{flushright}
The Information Technology Act, 2000 was amended in 2008 whereby India has become technologically neutral by adopting ‘electronic signatures’ as a means of authentication of an electronic record thus replacing the requirement of digital signatures as prescribed in the Information Technology Act, 2000. As authentication of any electronic record by a subscriber by means of the electronic technique specified in the II schedule and includes digital signatures. The II schedule containing e-signatures recognised by the Information Technology Act, 2000 are yet to be issued by Central Government till the time there are notified at least digital signatures are recognised as valid electronic signature under Information Technology Act, 2000. Under Section 3 of the Information Technology Act, 2000, the electronic records may be authenticated by affixing digital signatures based on the PKI system or other means of electronic signature which can be considered reliable. Section 3A of the Act specifies the criteria for assessing reliability of the electronic authentication technique. This is reliable if the signature creation data or the authentication data are linked to the signatory or the authenticator only and at the time of signing is solely under their control. In case any alteration is made to the electronic signature after affixing it, such alteration is detectable and any alteration to the information after its authentication by the electronic signatures is also detectable. The Central Government has been conferred with the power to prescribe the procedure to ascertain that the electronic signature is of a particular signatory. Section 4 of the Act confers legal recognition to electronic records and provides that whenever any law requires information in writing or in type written or printed form then such requirement shall be deemed to be satisfied if such information or matter is rendered or made available in electronic form and accessible so as to be usable for a subsequent reference. Section 5 recognises electronic signature which equates it with paper based signature when an electronic signature is affixed in a manner which is prescribed by the Central Government. Chapter V of the Information Technology Act, 2000 describes the meaning of ‘secure electronic record’ and ‘secure electronic signature’. Sections 14 and 15 speak about the security procedure. Section 14 of the Act stipulates that if any security procedure has been applied to an electronic record then it shall be deemed to be secure electronic record. Section 15 of the Information Technology Act provides that an electronic signature shall be deemed to be a ‘secure electronic signature’. If the signature
creation data at the time of affixing signature is solely under the control of signatory only and that the data was stored and affixed in such exclusive manner as prescribed by the central Government. In case of digital signatures ‘signature creation data’ refers to the private key of the signatory. Information Technology Amendment Act, 2008 inserted the word ‘secure electronic signature’ in place of secured digital signature. Under Section 16 of the Information Technology Act, 2000 power has been conferred to the Central Government to prescribe the security procedure and practices that shall be covered under Section 14 and 15 of the Information Technology Act, 2000. The Central Government shall consider ‘commercial circumstances’ nature of transactions and other connected factors – while prescribing the security procedures and practices. Here Central Government may consider Retina scanning, finger printing, iris scan to be secure electronic signature as it will be unique to the subscriber and remain within its exclusive control and can be easily affixed by even illiterate persons or those who are not technologically adapt to use sophisticated techniques such as digital signatures. These techniques will be more successful means of affixing digital signatures.\(^{102}\) This is found in the present ‘Aadhar’ card system, wherein biometrical retina scanning has gained vast acceptance among Indian population as a useful tool for authentication. Chapter VI of the Information Technology Act 2000 provides for the appointment of the controller who shall supervise over the activities of the Certifying Authorities and lay down the standards to be maintained by the certifying Authorities which is highlighted in the Information Technology Act, 2000 by virtues of Sections 16 and 17. By virtue of the 2008 amendment of the Act the Controller is no more the repository for digital signature certificate records. The Certifying Authority who is licensed to issue electronic signature certificates under Section 21 of the Information Technology Act, shall also maintain and update the records of the electronic signature certificate with effect from 27\(^{th}\) October 2009 specified in Section 20 of the Act.

India’s PKI Infrastructure hierarchy shows subscriber at the bottom most level, Certifying Authority just above them and finally the tip of the pyramid – the highest

control is the Controller. Indian Department of Telecommunication (DoT) prescribes encryption norms when granting license to the Internet Service Provider (ISP) to imbibe encryption mechanisms to ensure the integrity and security of the message transmitted. The Information Technology Act 2000 conferred power on the Controller to act as a repository of digital signature certificates. However by the Information Technology Amendment Act, 2008, this provision is repealed and provides that the Certifying Authorities shall be responsible to maintain correct records of digital signature certificates issued by it. Many regulations have been passed concerning the electronic signatures such as the Information Technology (Certifying Authorities) Rules 2000 as amended by the Amendment Rules 2009, the Information Technology (Certifying Authority) Regulations 2001, the Information Technology (Use of Electronic Records and Digital Signatures) Rules 2004, Information Technology (Security Procedure) Rules, 2004, Information Technology (Electronic Service Delivery) Rules 2011. These Rules regulate the functioning the Certifying Authorities explains the security procedure and prescribe provisions for use of electronic records and digital signatures. These rules also explains about the authentication procedure for creation and verification of digital signatures licensing of Certification Authorities and stipulate security guidelines for certification Authorities and guidelines for issue, term and revocation of digital signature certificate and governments delivery of services by electronic means. Apart from this Schedule II of Information Technology (Certifying Authority) Rules 2000 contains Information Technology security guidelines for organisations to develop internal processes in compliance with the requirements in the guidelines.

5.16.1 Cyber Appellate Tribunal Information Technology Act, 2000

Chapter X Sections 48 to 64 deals with the establishment of Cyber Appellate Tribunal. Section 48 stipulates that the Central Government shall by notification; establish one or more appellate tribunals which will be known as the Cyber Appellate Tribunal. Section 49 deals with the composition of the Cyber Appellate Tribunal, Section 50 mention the qualifications which the Chairperson and Members of the Cyber Appellate Tribunal should possess. Section 51 and Section 52 stipulate the Term of office, conditions of service etc., of the Chairperson and Members and Salary, allowances and other terms and conditions of Chairperson and Members respectively. Sections 52A
to 52D deal with the Powers of superintendence, direction, etc., Distribution of business among benches, Power of the Chairperson to transfer cases and Decision by majority. Section 53 of the Act speaks about the manner in which the vacancies in the tribunal must be filled up and Section 54 deals with the resignation and removal of the Chairperson and Members. According to Section 57 of the Information Technology Act, 2000 any person aggrieved by an order made by the controller has a right to prefer an appeal to the Cyber Appellate Tribunal. Section 58 enunciates the procedures and powers of the Tribunal.

Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a Judicial proceeding within the meaning of Sections 193 and 228 and for the purposes of Section 196 of the Indian Penal Code and Cyber Appellate Tribunal shall be deemed to be a Civil Court for the purpose of Section 195 and Chapter XXVI of the Code of Criminal Procedure 1973. It has powers including summoning, requiring, discovery and production of documents, receiving evidence an affidavit reviewing its decisions amongst other matters. A person aggrieved the order of the said tribunal can file an appeal to the High Court within 60 days from the decision of the Cyber Appellate Tribunal as per Section 62 of the Act. Further Section 64 of the Information Technology Act highlights about the recovery of penalty or compensation awarded if not paid the same shall be recovered as an arrear of land revenue and the license or the Electronic Signature certificate as the case may be shall be suspended till the penalty is paid. The word electronic signature was replaced in place of digital signature by virtue of Act 10 of 2009.

Chapter VI elucidates about the Regulation of Certifying Authorities appointment and Controller and other officers, functions of Controller and other officers, Recognition of foreign Certifying Authorities, Section 20 which stipulated that the controller is to act as repository has been repealed by the Information Technology Amendment Act 2008 – Section 13, License to issue Electronic Signature Certificates, Application for license, Renewal of License, Procedure for grant or rejection of
license,<sup>109</sup> Suspension of license,<sup>110</sup> Notice of suspension or revocation of license,<sup>111</sup> Power to delegate,<sup>112</sup> Power to investigate contraventions,<sup>113</sup> Access to computers and data,<sup>114</sup> Procedure to be followed by the Certifying Authority,<sup>115</sup> Certifying Authority to ensure compliance of the Act, etc.,<sup>116</sup> Display of license,<sup>117</sup> Surrender of license<sup>118</sup> and Disclosure.<sup>119</sup> Section 28 confers powers on the Controller to investigate any contraventions of the provisions of the Act or regulations and Section 29 confers powers on the controller to access any computer system, data on materials for the purpose of such investigation. Section 30 provides of such investigation. Certain procedures to be followed by the certifying authority are specified whereby every certifying Authority is required to maintain reasonable level of reliability in its services and make use of hardware, software and procedures which are secure from intrusion or misuse. The Certifying Authority is required to put in place adequate security procedure to ensure secrecy and privacy of electronic signatures which are maintained and those which perform the role of Repository for all electronic signature certificates. Sections 37 and 38 prescribe provisions for suspension of and revocation of digital signature certificates respectively. Section 42 of the Information Technology Act 2000 places the responsibility of maintaining confidentiality of the Private Key with the subscriber. In case this key is compromised the subscriber is liable till he has informed the Certifying Authority that his private key has been compromised.

From the above discussions it stands crystal clear that as far as electronic signature regime in India is concerned in unfolding as its basic legal framework has been

---

<sup>108</sup> Section 23 of the Information Technology Act, 2000
<sup>109</sup> Section 24 of the Information Technology Act, 2000
<sup>110</sup> Section 25 of the Information Technology Act, 2000
<sup>111</sup> Section 26 of the Information Technology Act, 2000
<sup>112</sup> Section 27 of the Information Technology Act, 2000
<sup>113</sup> Section 28 of the Information Technology Act, 2000
<sup>114</sup> Section 29 of the Information Technology Act, 2000
<sup>115</sup> Section 30 of the Information Technology Act, 2000
<sup>116</sup> Section 31 of the Information Technology Act, 2000
<sup>117</sup> Section 32 of the Information Technology Act, 2000
<sup>118</sup> Section 33 of the Information Technology Act, 2000
<sup>119</sup> Section 34 of the Information Technology Act, 2000
crafted well by the Information Technology Act and the subsequent rules framed provides more support and authenticity to the electronic transactions.

5.16.2 Role of the Information Technology Act, 2000 in Curbing Cyber Crimes

Having had an overview of the various cyber crimes and the ways in which we can protect ourselves from falling a prey the cyber attacks, there is a necessity to see how well our Information Technology Act, 2000 performs its role as a controller and watchdog of the cyber crimes. The virtual world has now become part and parcel of its real counterpart. Real world crimes are adequately addressed to and there are sufficient rules and regulations to control and curb them. The virtual world and the cyber space are recent developments and the crimes are also recent developments. The increased usage of the web, multibillion dollar transactions being just a click away, communications and social networking being made easy have led to the increase in the crime rate in the cyber space. The unscrupulous persons are taking advantage of either the innocence or ignorance of the users, try to extract money from them or just hack into their accounts and obtain unlawful gain. These are just offences committed with the intent to obtain an unfair or illegal gain at the expense of another. Offences are also committed to seek revenge. Posting pornographic material, defacing a web with intent to defame a firm or the government, posting pirated versions of music and movies etc., till the enactment of the Information Technology Act, 2000 the offences were dealt with under the Indian Penal Code. Certain provisions of the Code was amended owing to the developments in technology, however the Code did not prove to be effective when it came to the crimes or offences of the cyber space. Hence there arose the need to enact a law for the breach of law committed in the virtual world. In accordance with the United Nations general assembly resolution dated 30th January 1997 which passed the UNCITRAL Model Law on Electronic Commerce, the Indian Government enacted the Information Technology Act, 2000 and the same came into effect on the 17th of October 2000. The punishments provided for various crimes under the Act have been dealt with here under.

A) Posting of offensive messages:

Messages which are offensive to a particular religion, community, ethnic group or political party may be posted in a blog or a social networking site. Such messages might
have the effect of either inciting hatred in the minds of the people or communal clashes between two groups. In a country like India where there are diverse groups of people, there is a necessity to preserve the harmony amongst the people failing which communal riots and clashes are certain to breakout.

This offence is dealt with under Section 66A of the Information Technology Act in addition to Sections 153A and 153B of the Indian Penal Code.

Messages which outrage the modesty of a woman or defame her may be posted in a social networking site; such messages not only portray her as a woman of bad character but also have a defaming effect on her. Such offences are dealt with under Sections 66A and 67 of the Information Technology Act. Other messages of defamation, in addition to Section 500 of the Indian Penal Code, are also governed by Section 66A of the Information Technology Act, 2000. Convictions under Section 66A and 67 are punished with an imprisonment which may extend up to a term of 3 years and fine and imprisonment for either description for a term which may extend up to 3 years and a fine of up to five lakh rupees for the first conviction and a fine of up to ten lakh rupees for the subsequent convictions.

A) Hacking:

Emails have now become the common mode of communication amongst people. The password of the email account holders may be hacked for several reasons, depending upon the reasons for which they are being hacked the offenders are dealt with under Sections 43, 66, 66A, 66C or 66D of the Information Technology Act, 2000 (amendment 2008).

In case a victim whose email has been hacked has been misused for sending out malicious code like viruses, Trojans, etc., or to extort money from the victim by threatening him, the offender will be penalised under sections 43, 66, 66A and 66C of the Information Technology Act. If the hacked email is used to send out obscene emails the offender is booked under Sections 67, 67A and 67B of the Information Technology Act in addition to the above mentioned sections. Section 43 stipulates that the offender may be made liable to pay compensation by way of damages. Convictions under Section 66 and 66A may subject the offender to imprisonment which may extend to a term of up to 3 years or fine which may extend to five lakh rupees or both and imprisonment for a term which may extend up to a
term of 3 years or fine respectively. Convictions under Section 66C and 66D are penalised with an imprisonment of either description for a term which may extend up to three years or fine which may extend up to rupees one lakh. Sections 67 prescribes a punishment of imprisonment of either description for a term of up to three years and a fine of up to rupees five lakhs for the first conviction and imprisonment of either description for a term of up to five years and a fine of up to rupees ten lakh for the subsequent conviction. Convictions under Sections 67A and 67B are penalised with an imprisonment of either description for a term of up to five years and a fine of up to ten lakh rupees for the first conviction and an imprisonment of either description for a term of up to seven years and a fine of up to ten lakh rupees for the subsequent conviction.

B) Credit Card and Online Share Trading Fraud:

Credit cards are now commonly used for online transactions. Inspite of the increase in the security measures implemented by e-commerce websites, there is also an increase in the instances of credit card frauds. In instances of credit card fraud cases the victims credit card information is stolen and misused for making online purchases. The information may be obtained by either installing key loggers in public computers or by noting down of the card details by workers at retail outlets, petrol pump attendants, hotel waiters etc.,

Post the dematerialisation of shares in India, it has become mandatory for investors to have demat accounts. In most cases the online banking account is linked with the online share trading account. Owing to this there have been many online share trading frauds. A victim’s account password may be stolen and misused for making fraudulent bank transfers or for making unauthorised transactions which would result in the losses to the victim.

Such offences are penalised under Sections 43, 66, 66C, 66D of the Information Technology Act and Section 420 of the Indian Penal Code. Section 43 stipulates that the offender may be made liable to pay compensation by way of damages. Convictions under Section 66 may subject the offender to imprisonment which may extend to a term of up to 3 years or fine which may extend to five lakh rupees or both. Convictions under Section 66C
and 66D are penalised with an imprisonment of either description for a term which may extend up to three years or fine which may extend up to rupees one lakh.

C) Source Code Theft:

A source code is the very foundation on which the software companies are built. A source code is the programming instructions that are compiled into executable files that are sold by software development companies.\textsuperscript{120} Source code theft most common in software companies; however it is not alien to banks, manufacturing companies or organisations which get original software developed for their use. In the event of source code theft, the offender is usually an employee of the victim for it is he/she who has direct or indirect access to the source code. The offender may use the stolen source code to either contact potential buyers and make a sale or modify the source code and make his own version of the software and sell it to prospective buyers. In either case the offence is punishable under Sections 43, 65, 66 and 66B of the Information Technology Act and Section 63 of the Copyright Act.

Section 43 stipulates that the offender may be made liable to pay compensation by way of damages. Convictions under Sections 65 and 66 may subject the offender to imprisonment which may extend to a term of up to three years or fine which may extend to two lakh rupees or both and imprisonment which may extend to a term of up to three years or fine which may extend to five lakh rupees or both respectively. Convictions under Section 66B may subject the offender to imprisonment of either description which may extend to a term of up to three years or fine which may extend to one lakh rupees or both.

D) Theft of Confidential Information:

Business organisations store their sensitive information in computer system. This information is target of rivals, criminals or disgruntled employees. A business rival may attempt to obtain this sensitive information and use it to an unfair advantage over the victim. A criminal may obtain this confidential information and subsequent to the receipt/extort money from the victim by threatening to make the information public unless his

\textsuperscript{120} Asian School of Cyber Laws – “Cyber Crime and Digital Evidence- An Indian perspective” Version 4 (Nov 2009)
demand is met with. An employee who has a strained relationship with his employer in order to seek his revenge may steal confidential information and mass mail it or sell it out to the victims rivals. This offence is penalised under Sections 43, 66 and 66B of the Information Technology Act.

Section 43 stipulates that the offender may be made liable to pay compensation by way of damages. Convictions under Section 66 and 66B may subject the offender to imprisonment which may extend to a term of up to 3 years or fine which may extend to five lakh rupees or both and imprisonment of either description which may extend to a term of up to three years or fine which may extend to one lakh rupees or both respectively.

E) Piracy:

It’s common notion among people to not consider software, music and video piracy as theft. People usually go in the pirated versions of the software, music or video they fail to realise that they are also properties and theft of them is also an offence. Piracy in music is a huge business now and pirated music can be purchased at throw away prices. The pirated versions may either be sold through physical media i.e., by CD ROMs etc or through electronic downloads through websites, bulletin boards, news groups, spam emails etc., This offence is penalised under Sections 43 and 66 of the Information Technology Act in addition to Section 63 of the Copyright Act. Section 43 stipulates that the offender may be made liable to pay compensation by way of damages. Convictions under Section 66 may subject the offender to imprisonment which may extend to a term of up to 3 years or fine which may extend to five lakh rupees or both.

F) Email Scams:

These scams are most commonly referred to as the Nigerian 419 scam. However research shows that very few of these emails actually originate in Nigeria. In these scams the suspect mails victim stating that he is going to get a lot of money (usually by way of winning a lottery). The suspect then sends some mails have official looking documents as attachments in order to convince the victim. Subsequent to this he asks the unsuspecting victim for a small fee to cover legal expenses and courier charges. If the victim pays the money all further contact is severed by the offender. The offender is charged under
Sections 66A and 66D of the Information Technology Act in addition to Section 420 of the Indian Penal code.

Convictions under Section 66A and 66D are penalised with imprisonment for a term which may extend up to 3 years or fine and an imprisonment of either description for a term which may extend up to three years or fine which may extend up to rupees one lakh respectively.

G) Phishing:

Sensitive information is acquired fraudulently by the offender by masquerading himself to be a trusted entity. A victim usually receives an email appearing to have been sent from his bank and urges him to click on the link in the email. When he does so the victim is taken to what appears to be a secure page on the bank’s website; while in reality it is actually a fake website which asks the victim to enter his username and password. Once the victim enters his information it is stolen and the account of the victim is then misused. Sections 66, 66A and 66D of the Information Technology Act deal with it in addition to Section 420 of the Indian Penal Code.

Convictions under Section 66 may subject the offender to imprisonment which may extend to a term of up to 3 years or fine which may extend to five lakh rupees or both. Convictions under Section 66A and 66D are penalised with imprisonment for a term which may extend up to 3 years or fine and an imprisonment of either description for a term which may extend up to three years or fine which may extend up to rupees one lakh respectively.

H) Cyber Pornography:

Cyber pornography includes pornographic websites, pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc). An offender accepts online payments and allows paying customers to view or download pornographic pictures,
videos etc from his website. Section 67 of the Information Technology Act applies. Section 67A and 67B may also apply.

Sections 67 prescribes a punishment of imprisonment of either description for a term of up to three years and a fine of up to rupees five lakhs for the first conviction and imprisonment of either description for a term of up to five years and a fine of up to rupees ten lakhs for the subsequent conviction. Convictions under Sections 67A and 67B are penalised with an imprisonment of either description for a term of up to five years and a fine of up to ten lakh rupees for the first conviction and an imprisonment of either description for a term of up to seven years and a fine of up to ten lakh rupees for the subsequent conviction.

I) Cyber Terrorism:

Terrorists use the real as well as the virtual world in order to hide information and records of their illicit business. Emails and chat rooms are widely used as mediums of communication amidst them. In addition to physical storage mediums like CD ROMs, DVD ROMs, pen drives, memory cards etc., they also use the virtual storage media like email accounts, online brief cases, FTP sites, Gspace etc., The terrorists also purchase and use encryption software to protect their information. The Information Technology Act penalises cyber terrorism under Section 69. In addition to the conventional terrorism laws also apply.

Convictions under Section 69 are punished with imprisonment of a term which may extend up to seven years and shall also be liable to fine.

J) Virus attacks:

A computer or network is infected with a virus which then destroys all the electronic information. With the increase in digitisation viruses are becoming a great threat to the digital world. A virus may either be a general ‘in the wild’ virus or a particular virus which targets only a particular organisation. Virus attacks are punished under Sections 43, 66 and 66A of the Information Technology Act and in addition are also dealt with under Section 426 of the Indian Penal Code.

Section 43 stipulates that the offender may be made liable to pay compensation by way of damages. Convictions under Section 66 may subject the offender to imprisonment which may extend to a term of up to 3 years or fine which may extend to five lakh rupees.
or both. Convictions under Section 66A are penalised with imprisonment for a term which may extend up to 3 years or fine.

K) Web Defacement

The substitution of the original home page of a website with another page by a hacker is web defacement. The most common targets of web defacement are religious and political websites. Disturbing images and offensive phrases are displayed in the process. In some occasions the defaced page also shows who was responsible for such defacement. The offence is charged under Sections 43 and 66 of the Information Technology Act. In some occasions charges are also framed under Sections 66F, 67 and 70 of the Information Technology Act.

Section 43 stipulates that the offender may be made liable to pay compensation by way of damages. Convictions under Section 66 may subject the offender to imprisonment which may extend to a term of up to 3 years or fine which may extend to five lakh rupees or both. If convicted under Section 66F, the offender shall be sentenced to an imprisonment which may extend to life. Sections 67 prescribes a punishment of imprisonment of either description for a term of up to three years and a fine of up to rupees five lakhs for the first conviction and imprisonment of either description for a term of up to five years and a fine of up to rupees ten lakhs for the subsequent conviction. Convictions under Section 70 are punished with an imprisonment of either description for a term which may extend up to ten years and shall also be liable to fine.

5.16.3 Effect of the penal provisions:

The offenders in the virtual world are usually white collared criminals. They often know the nuances of committing a computer crime without getting caught. It is usually said that if one is a good hacker everyone will know his name however if he is a great hacker no one will know who he is. With the increase in the cyber crime rates there is a necessity to increase the security measures which are involved too. In order to curb the cyber crimes a fool proof system is mandatory. However in addition to that effective penal provisions are also needed. It is these penal provisions which act as a deterrent for further commissions of the offences. These penal provisions have the deterrent effect for white collared or the educated lot of the population look at a conviction as a disgrace to
them the society usually looks down upon them. No educated person from a respectable background would want to be in such a situation. Thus we could say that the penal provisions of the Information Technology Act not only offer punishments to the convicts but also has the deterrent effect, which prevents future offences.

5.16.4 Conclusion

The Information Technology Act 2000 has brought amendment in four statutes vide Sections 91 to 94, which have been provided in Schedules 1 to 4. Sections 91, 92, 93 and 94 stipulate that The Indian Penal Code shall be amended in the manner specified in the I Schedule of the Act, The Indian Evidence Act shall be amended in as specified in the II Schedule of the Act, The Bankers Book Evidence Act 1891 shall be amended as specified in the III Schedule and The Reserve Bank of India Act, 1934 shall be amended as per the IV Schedule respectively.

In order to take the best advantage of the fast cost effective method of securities trading offered over the Internet the SEBI (Securities Exchange Board of India) issued the guidelines on 31st January 2000 for Internet based securities trading and services. For legal purposes the Information Technology Act, 2000 is applicable to all electronic contracts and transactions entered into under the SEBI guidelines. In the same manner RBI issued Internet banking guidelines on the 14th of June 2001. India has legally recognised Internet Banking and with an increase in awareness among the masses and with the development of an infrastructure to support Internet banking a shift from the traditional modes of banking to Internet banking is predicted in the near future. The Information Technology Act has catered to the various requirements to enable electronic transactions to be safe and secure. However few limitations of the Information Technology Act, 2000 are: the Foreign Certifying Authorities were also recognised under Section 19 of the Act. Certain drawbacks were identified in these sections when the Foreign Certifying Authorities are already recognised then it is embarrassing to ask them to obtain a license from the Central Government once again. Foreign Certifying Authorities should be subjected to licensing only if they want to issue digital certificates to individuals or companies in India. But say if the foreign company wants to step up digital certificate services in India but does not have recognition in any other country then
such companies may be subjected to prior approval of Government and Gazette notification. Information Technology Act has not brought out the provisions which can be applicable to Negotiable Instruments Act 1881 and Indian Trust Act, 1882.

Information Technology Act only recognises PKI framework for authentication and does not recognise any other form of authentication procedures. Next search and powers of arrest conferred on the police officers are specific to public places, while guidelines are provided for such powers in other locations. Information Technology Act is a comprehensive piece of legislation which aims at policing some activities over the Internet. The fundamental approach of the Act is towards validating and legalising electronic and online transactions. Business transactions’ cost has been tremendously reduced and profits have grown voluminously. However the working and implementation of this law will depend greatly on the rules and regulations that will be formed by the Government and other authorities constituted under the Act.

The Act is a skeletal figure and its regulations will form the fleshy content. The Act is only a beginning of legislation that still needs to be formed and implemented. The infrastructure and administrative needs, commercial acceptance of e-signatures, user viability issues, cross certification propositions and technical robustness of e-signatures against identity thefts damage or tampering will need to be tested by the passage of time. This chapter explains the prescription of a security procedure for online transactions which amounts to giving recognition to the PKI Infrastructure under the current technological developments at the security level. The chapter has emphasised the statutory creation of Certifying Authority and the regulatory body namely the controller of Certifying Authorities and the Appellate body Cyber Regulations Appellate Tribunal. It is emphasised that the creation of these statutory bodies has contributed to the certainty and finality of E-commerce legislation in India. It is time to face the reality, because electronic transactions are becoming inevitable and Digital Security has to be strengthened. Identity theft, corporate security breaches and an increased interest in personal privacy are forcing changes like changing the passwords more often with stronger ones. Security experts say email is a lot more like a postcard than a letter insider an envelope, and almost anyone can read it while it is in transit. The best way to do this is with a process known as encryption, which scrambles a message into unreadable code that needs a key to be
unlocked providing a layer of protection if someone intercepts the email. Many new tools are arriving regularly that should make it easier to encrypt email. The latest promising new encryption tool is virtue a feature that can be added to Chrome and Fire Fox browsers. The researcher is of the opinion that the security threats posed by the advance development in science and technology are being rectified or other alternative measures are being taken to protect the users of the internet. It is high time that legislators take enough steps to enact legislations and amend the IT Act as cyber offences surface in any format anytime. Law should very much try to cope up with the technology.

122 The Times Of India, Coimbatore, Bennet Coleman & Co. Ltd. Friday, July 18th 2014, Vol.3, issue 278 p.11