INTRODUCTION

This introductory chapter deals with meaning of cyber crimes, cyber terrorism, the nature and the causes of such crimes, objectives, methodology and the rationale of the study with chapter design. The present research study aims at detailed investigation of the emerging cyber-crimes and also proposes methods to control this ever increasing crime. The sociological impact of the crime would also form the part of this study although the study covers the economic and legal dimensions and thus, inter-disciplinary in nature. The study would also estimate the effectiveness of existing cyber laws. The study would analyze and collect the committed cyber crimes and study its operation and its sociological effects.

Conceptualization of cyber crime:

Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is “a legal wrong that can be followed by criminal proceedings which may result into punishment.” The hallmark of criminality is that, it is breach of the criminal law. A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

According to B. Muthukumaran (2008) “Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. Today e-mail and Websites have become the preferred means of communication. Organizations provide Internet access to their staff. By their very nature, they
facilitate almost instant exchange and dissemination of data, images and variety of material. This includes not only educational and informative material but also information that might be undesirable or anti-social”.

To understand cyber crime as a significantly new phenomenon, with potentially profoundly new consequences, it is necessary to recognize it as a constituent aspect of wider political, social and economic reconstructing currently effecting countries world wide. This new technology not only provides opportunities for the profitable development of an international information market but has also raised the specter of new criminal activities to exploit them. The very technology that enables multinationals to do business more effectively and challenge the individual controls and regulations of nation states, also offers the prospect of globally organized criminal networks. Moreover, the free flow of uncensored information on electronic networks and websites is as attractive to insurgents and extremists groups as it is to dissidents proclaiming their human rights. Just as crimes have changed with the growth of information technology so have the categories of criminals who engage in such crimes, ranging from hackers, information merchants and mercenaries, to terrorists, extremists and deviants.

Cyber crimes are any illegal activities committed using computer target of the criminal activity can be either a computer, network operations. Cyber crimes are genus of crimes, which use computers and networks for criminal activities. The difference between traditional crimes and cyber crimes is the cyber crimes can be transnational in nature. Cyber crime is a crime that is committed online in many areas using e-commerce. A computer can be the target of an offence when unauthorized access of computer network occurs and on other hand it affects e-commerce. Cyber crimes can be of various types such as telecommunications piracy, electronic money laundering and tax evasion, sales and investment fraud,
electronic funds transfer fraud and so on so forth.

Cyber crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime". "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime".

A generalized definition of cyber crime may be "unlawful act wherein the computer is either a tool or target or both". The computer may be used as a tool in the following kinds of activity: financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases: unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

Cyber crime began with such discontented employees causing physical damage to the computers they worked with to get back at their superiors. As the ability to have personal computers at home became more accessible and popular, cyber criminals began to focus their efforts on home users. The most common cyber crimes during this time were phishing scams, cyber stalking, computer viruses, and identity theft. As the years went on and more and more households bought home computers with Internet access, cyber crime became bigger and much harder to control. Cyber stalking and harassment also became far more popular. Middle school and high school kids began to take advantage of the Internet to taunt their classmates and adults would stalk and harass those they also stalked in
real life via the internet. Police departments and federal law enforcement have created special divisions specifically to deal with cyber crime. However, by judging the history of cyber crime, it is clear that it is not going to stop anytime soon and it seems like it will just continue to grow until new methods of fighting it are introduced.

Cyber crime is an evil having its origin in the growing of dependence on computers in modern life. Cyber crime is addressed in the broadest sense, in a way that most emerging crimes today involve the use of information technology. The terms 'Computer Crime', 'Computer Related Crimes', 'Internet Crime', 'Online Crimes', 'Hi-Tech Crimes', 'Information Technology Crime', and 'Cyber Crimes' are being used interchangeably. Computer crime can involve criminal activities that are traditional in nature such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a new age of crimes that are addressed by the Information Technology Act, 2000.

Defining cyber crimes, as “acts that are punishable by the Information Technology Act” would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as e-mail spoofing and cyber defamation, sending the threatening e-mails, etc. A simple definition of cyber crime would be “unlawful acts wherein the computer is either a tool or a target or both”.

In brief, the term cyber crime is usually restricted to describing criminal activity in which the computer or networks is an essential part of the crime and the term is also used to include traditional crimes in which computers or networks are applied to enable illicit activity. The word "cyber" first came into recognition when the novelist William Gibson used the term in his novel "Neuro-Mancer" to describe the imaginary space in which cyber criminals like "Hackers" operated. As a recent report from the
Center for Strategic and International Studies stated, cyber crime "is the organized crime of the twenty-first century."

The word cyber and its relative dot.com are probably the most commonly used terminologies of the modern era. In the information age the rapid development of computers, telecommunications and other technologies has led to the evolution of new forms of transnational crimes known as "cyber crimes". Cyber crimes have virtually no boundaries and may affect every country in the world. In a simple parlance they may be defined as "any crime with the help of computer and telecommunication technology" with the purpose of influencing the functioning of computer and the computer systems.

The Oxford Reference online defines cyber crime as crime committed over the Internet. The Encyclopedia Britannica defines cyber crime as any crime that is committed by means of special knowledge or expert use of computer technology. Cyber crime could reasonably include a wide variety of criminal offences and activities. The scope of this definition becomes wider with a frequent companion or substitute term "computer-related crime." Examples activities that are considered cyber crime can be found in the United Nations Manual on the Prevention and Control of Computer Related Crime. The manual includes fraud, forgery, computer sabotage, unauthorized access and copying of computer programs as examples of cyber crime. Malaysia was amongst the first few countries in the world to introduce cyber laws.

United Nations' Definition of Cyber crime:

Cyber crime spans not only state but national boundaries as well. At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cyber crime was broken into two categories and defined thus:
Cyber crime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

Cyber crime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network. Of course, these definitions are complicated by the fact that an act may be illegal in one nation but not in another.

There are more concrete examples, including

- Unauthorized access
- Damage to computer data or programs
- Computer sabotage
- Unauthorized interception of communications
- Computer espionage

These definitions, although not completely definitive, do give us a good starting point one that has some international recognition and agreement for determining just what we mean by the term cyber crime.

The development of information technology and the widening usage of the Internet have made it possible for cyber crimes to take place. Some people argue that cyber crime gives advantages to certain individuals because it gives them an opportunity to enhance their computer skills and make a profit out of it. However, that is far from truth. In reality, cyber crime kills e-commerce industry as seen through the unleashing of viruses, fraud, and variety of tools available on the net and unauthorized use of computers.

Cyber crime is hard to detect, thus giving the perpetrators ample of time to escape the area in which the crime was committed, because of this fact the criminals can be in another country far away from the scene of the
crime by the time it is detected. Cyber crimes differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

Reasons for cyber crime:

Hart in his work "The Concept of Law" has said 'human beings are vulnerable so rule of law is required to protect them'. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime. The reasons for the vulnerability of computers may be said to be:

**Capacity to store data in comparatively small space:**

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.

**Easy to access:**

The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is frail and it is not possible that there might not be a slip at any stage. The cyber criminals take advantage of these lacunae and penetrate into the computer system.

Negligence is very closely connected with human conduct. It is
therefore very probable that while protecting the computer system there
might be any negligence, which in turn provides a cyber criminal to gain
access and control over the computer system. Loss of evidence is a very
common and obvious problem as all the data are routinely destroyed.
Further collection of data outside the territorial extent also paralyses this
system of crime investigation.

Modus operandi of cyber crime:

Unauthorized access to computer systems or networks / Hacking:

This kind of offence is normally referred as hacking in the generic
sense. However the framers of the Information Technology Act 2000 have
no where used this term so to avoid any confusion we would not
interchangeably use the word hacking for ‘unauthorized access’ as the latter
has wide connotation.

Theft of information contained in electronic form:

This includes information stored in computer hard disks, removable
storage media etc. Theft may be either by appropriating the data physically
or by tampering them through the virtual medium.

E-mail bombing:

This kind of activity refers to sending large numbers of mail to the
victim, which may be an individual or a company or even mail servers there
by ultimately resulting into crashing.

Data diddling:

This kind of an attack involves altering raw data just before a
computer processes it and then changing it back after the processing is
completed. The Electricity Board faced similar problem of data diddling
while the department was being computerised.
Salami attacks:

This kind of crime is normally prevalent in the financial institutions or for the purpose of committing financial crimes. An important feature of this type of offence is that the alteration is so small that it would normally go unnoticed.

Denial of Service attack:

The computer of the victim is flooded with more requests than it can handle which cause it to crash. Distributed Denial of Service (DDoS) attack is also a type of denial of service attack, in which the offenders are wide in number and widespread e.g. Amazon, Yahoo.

Virus/worm attacks:

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

Logic bombs:

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. Even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

Trojan attacks:

This term has its origin in the word ‘Trojan horse’. In software field this means an unauthorized programme, which passively gains control over another’s system by representing itself as an authorised programme. The
most common form of installing a Trojan is through e-mail e.g. a Trojan was installed in the computer of a lady film director in the U.S. while chatting. The cyber criminal through the web cam installed in the computer obtained her nude photographs. He further harassed this lady.

**Internet time thefts:**

Normally in these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password e.g. Colonel Bajwa’s case - the Internet hours were used up by any other person. This was perhaps one of the first reported cases related to cyber crime in India. However, this case made the police infamous as to their lack of understanding of the nature of cyber crime.

**Web jacking:**

This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money e.g. recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein. Further the site of Bombay crime branch was also web jacked. Another case of web jacking is that of the ‘gold fish’ case. In this case the site was hacked and the information pertaining to gold fish was changed. Further, a ransom of US $1 million was demanded as ransom. Thus, web jacking is a process where by control over the site of another is made backed by some consideration for it.

**Harassment via e-mails:**

Harassment through e-mail is not a new concept. It is very similar to harassing through letters. Recently, a mail has been received from a lady wherein she complained about the same. Her former boy friend was
sending her mails constantly sometimes emotionally blackmailing her and also threatening her. This is a very common type of harassment via e-mails.

**Cyber-stalking:**

The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with e-mails etc.

**Dissemination of obscene material/ Indecent exposure/ Pornography (basically child pornography) / Polluting through indecent exposure:**

Pornography on the net may take various forms. It may include the hosting of web site containing these prohibited materials. Use of computers for producing these obscene materials, downloading through the Internet, obscene materials is some of the instances of this category of crimes. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind. Two known cases of pornography are the Delhi Bal Bharati case and the Bombay case wherein two Swiss couple used to force the slum children for obscene photographs. The Mumbai police later arrested them.

**Defamation:**

It is an act of imputing any person with intent to lower the person in the estimation of the right-thinking members of society generally or to cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium e.g. the mail account of a boy was hacked and some mails were sent from his account to some of his batch mates regarding his affair with a girl with intent to defame him.
Unauthorized control/access over computer system:

This activity is commonly referred to as hacking. The Indian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking" to prevent confusion as the term used in the Act of 2000 is much wider than hacking.

Computer vandalism:

Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.

Intellectual Property crimes / Distribution of pirated software:

Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived of completely or partially of his rights is an offence. The common form of Intellectual Property Right (IPR) violation may be said to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc. In one such incident the Hyderabad Court has in a landmark judgement has convicted three people and sentenced them to six months imprisonment and fine of 50,000 each for unauthorized copying and sell of pirated software.

Cyber terrorism against the government organization

We need to explain the difference between cyber terrorism and cyber crime. Both are criminal acts. However there is a compelling need to distinguish between both these crimes. A cyber crime is generally a domestic issue, which may have international consequences; however cyber terrorism is a global concern, which has domestic as well as international
consequences.

The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks, etc. Technology savvy terrorists are using 512-bit encryption, which is next to impossible to decrypt. The recent example may be cited of - Osama Bin Laden, the LTTE, and attack on America’s army deployment system during Iraq war.

Cyber terrorism may be defined to be “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” Another definition may be attempted to cover within its ambit every act of cyber terrorism.

A terrorist means a person who indulges in wanton killing of persons or in violence or in disruption of services or means of communications essential to the community or in damaging property with the view to putting the public or any Section of the public in fear; or affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or coercing or overawing the government established by law; or endangering the sovereignty and integrity of the nation. A cyber terrorist is the person who uses the computer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof is an act of cyber terrorism.

Trafficking:

Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms weapons etc. These forms of trafficking are going unchecked because they are carried on under pseudonyms. A racket was busted in Chennai where drugs were being sold under the pseudonym of honey.
Fraud and Cheating:

Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc. In one of the cases, the Court of Metropolitan Magistrate Delhi (17) found guilty a 24-year-old engineer working in a call centre, of fraudulently gaining the details of Campa's credit card and bought a television and a cordless phone from Sony website.

The emergence of internet crimes in the law

The internet has opened up a world of new opportunity for gender activists and development actors working in the arena of information and communications technologies (ICT). The need for access, connectivity and relevant content has been well argued by researchers and advocates alike, but as the reach of the internet expands, new issues arise in bridging the 'digital divide'. Invasions of privacy, objectionable and malicious content, cyber harassment and other forms of cyber crimes undermine the Internet's potential as a greater equalizer and threaten autonomy and security of individuals, organizations and communities, and nations.

United Nations Commission on Trade Law as a consequence of which the information Technology Act 2000 was passed and enforced on 17th May 2000. The preamble of this Act states its objective to legalize e-commerce and further amend the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker's Book Evidence Act 1891 and the Reserve Bank of India Act 1934. The basic purpose to incorporate the changes in these Acts is to make them compatible with the Act of 2000. It was believed that these laws will facilitate to regulate and control the affairs of the cyber world in an effective manner.

The Information Technology Act deals with the various cyber
crimes in chapters IX and XI. The important Sections are 43, 65, 66, 67. Section 43 in particular deals with the unauthorized access, unauthorized downloading, virus attacks or any contaminant, causes damage, disruption, dental of access, interference with the service availed by a person. This Section provide for a fine up to Rs. 1 crore by way of remedy. Section 65 deals with "tampering with computer source documents" and provides for imprisonment up to 3 years or fine, which may extend up to 2 years or both. Section 66 deals with "hacking" with imprisonment up to which may extend up to 2 years or both. Further Section 67 deals with publication of obscene material and provides, for imprisonment up to a term of 10 year: and also with fine up to Rs. 2 lakhs.

Chapter XI of India's Information Technology (IT) Act defines cyber crime offenses as: tampering with computer source documents; hacking; publishing of information which is obscene in electronic format; breaching of confidentiality; and publishing false digital signatures. Yet as the Internet has evolved drastically and often in unanticipated directions in the Years since the IT Act was passed in 2000, so has the nature and severity of cyber crime.

A typology of cyber crimes reveals that most crimes fall into three categories: crimes committed against persons, crimes committed against property and crimes committed against governments. Crimes of the first category have particularly captured the attention of the Indian news media and public, and generated considerable discussion on the need for more safety measures and increased regulation of the internet. As policy makers are called upon to respond, it becomes critical to consider how cyber crime and the emergent legislation will have impact on the social, economic and political participation of women and other marginalized groups.

**Objectives of the study:**

The year 2011 has witnessed a quantum jump not only in the
quantity and quality also the very nature of cyber crime activities. As opposed to obscenity, pornography, malicious e-mails that were more prevalent in the past, now credit card frauds, phishing attacks, online share trading, etc. are becoming more widespread. Therefore, there is an imperative need to examine the legislative measures to curb such crimes and to maintain the information security. Despite the enactments of plethora of acts and legislations, how we con implement such measures to control the crimes is an important issue of concern. For instance, the United States has several, including the Computer Fraud and Abuse Act (1986), the Computer Misuse Act. (1991), the Electronic Fund Transfer Act (1991), the Electronic Fund Transfer Act (1996) and the Child Online Protection Act (1998). It is just possible that the volume and nature of cyber crime in our country would demand in course of time a multiplicity of such laws. Apart from private digital enterprises, law enforcement agencies including the Central Bureau of Investigation (CBI) the Enforcement Directorate, the Directorate of Revenue Intelligence and the Income Tax Investigation Wing, could provide valuable inputs to the government. There is also the need to draw from the international experience. For instance, the Council of Europe recently agreed on certain parameters with a view to ensuring uniformity in cyber law. The Interpol is also active on this front and may be help to ensure that our law does not ignore new developments.

Like most of modern crime, cyber crime knows no boundaries. A hacker in Albania can break into a system in Kanyakumari without the aid of any extraordinary talent or equipment. A personal computer is all that he or she will need. Software of a mind-boggling variety is available for this operation and there is any number of websites to offer information. The ease with which such cyber vandalism can be committed has helped build an international consensus that a hacker should not be allowed to get away only because of legal inadequacies. Section 75 of the IT Act clearly lies down that its provisions shall also apply to "any offence or contravention
committed outside India by any person, irrespective of his nationality", provided that such act involves a computer, a computer system or computer network located in India.

The Commission on Crime Prevention and Criminal Justice (CCPCJ) of the United Nations, with its headquarters in Vienna, has been exercised over how to prevent and control high technology and computer related crime. The Commission is convinced that one way of doing this is to forge closer links between nations so that the cyber criminal is relentlessly pursued across frontiers.

The U.N. Convention on Transnational Organized Crime adopted by the General Assembly on November 15, 2000 may not directly apply to routine computer crime. However, it will definitely be attracted where organized gangs use telecommunication and computer networks for their operations. Following this Convention, the CCPCJ held a workshop on “The Challenge of Borderless Cyber Crime” in December 2000 at Palermo, Italy. The workshop, attended by representatives of a large number of countries gave a fillip to the movement that aims to strengthen the law and procedure for international cooperation in the field.

The Lyon Group of high level experts set up by the G-8 nations has also been active. At this group's instance, a network of contacts available round-the-clock has been established. The Interpol has now the operational responsibility for this network and the CBI has been identified as a contact point for the Indian subcontinent and its neighbourhood.

In view of the severity of the issues involved in such acts of crime, the present study has been proposed with the following objectives:

1. To discuss at length the nature and the causes of such crimes, objectives, methodology and the scheme of the present study,

2. To outline nature, classification and dimension of cyber crime and to focus on some of the cases of cyber crimes in India,
3. To examine the socio-economic impact of cyber crime with the help of available secondary sources of materials,

4. To present an evaluative study of legislative measures and provisions to combat such crimes, and

5. Finally, to present the concluding observations and to suggest remedial measures to curb such crimes

**Methodology**

Keeping the objectives of the study in view, the present research study has been undertaken with the help of empirical research tools. The collection of data would be done from available books, articles, conference reports and also taking interviews of the concerned people who are responsible to implement the laws to mitigate such crimes. Therefore, the methodology would involve a synthesis of primary and secondary sources to be documented in the descriptive analysis.

We were ascertained and the investigation have revealed share frauds; credit card crime, financial thefts etc. Indian Detective Agency can detect and help prevent such crime by providing a complete package to counteract related frauds and abuses. The interviews of the authorities responsible for lodging complaints of cyber crime made it possible to record all about the reported cyber crimes. It is revealed that unreported cyber crime surpasses the actual numbers of cases. Interviews of Yahoo Mail and Hotmail, MSN India Representative offices in India having responsibility as service providers for any Cyber Crime committed in India under Information Technology Act-2000 or other laws would also provide information on detection, identification, curtailment and prevention of cyber crime.

The case studies have been selected from the reported cyber crimes. The interviews would include the officials responsible for control and detection of cyber crime. This includes the various officials
of CBI, police and Special Task Force and Cyber Cells. The Bank officials engaged in electronic banking would also be interviewed. The office of the local web sites have been consulted and interviewed. The sufferers of the cyber crime have been enlisted for interview. To trace the sociological impact and cause of cyber crimes the interviews of cross Section of the society have been taken.

Justification of the study:

Today an increasing number of companies are connecting to the Internet to support sales activities or to provide their employees and customers with faster information and services.

The modern world relies on computerized system for almost every thing in the life, from air, train and bus traffic control to medical services. The rapid expansion of large-scale computer networks and the ability to access systems through regular telephone lines increase the vulnerability to these systems. The virtual world has taken over the real one, e-business and e-commerce, which are the new mantras and electronic transactions and dominate the overall business paradigm.

Modern business is quickly replacing cash with deposits transacted on computer system creating computer fraud. Credit card information as well as personal and financial information on credit card has been frequently targeted by organized criminal crimes. Intangible assets represented in data format such as money on deposits or hours of work are the most common targets related to fraud. Assets represented in data format often have a considerably higher value than traditionally economic assets resulting in potentially greater economic class. Computers however can also be used as instruments for committing forgery. A new generation of fraudulent alteration or duplication emerged when computerized color laser copies became available. These copies are capable of high-resolution copying, modification of documents that are even creating false documents
without benefit of original. They produce documents with an equality that is indistinguishable from original documents. In this rapidly evolving e-world that depends on free flowing information, security is the major problem to be considered. Security on Internet is challenging. Security on an Internet is important because information has significant value. Implementing security involves assessing the possible threats to one’s network, servers and information.

In the light of the above-analysis, there is a rationale to understand the problem of cyber crimes, its magnitude and dimensions and to minimize the threat as much as possible. Therefore, the present study of understanding the nature, extent and the impact of sociological and economic aspects of cyber crime is of immense significance. This piece of research work is therefore, a pioneering effort to help expand the knowledge base on the act of cyber crimes thereby assisting people to be more careful about their information, money in the bank and other valuables.

**Schemes of the study:**

The present study has been documented in the following chapters:

Chapter-1: Introduction

Chapter-2: Review of Literature

Chapter-3: Nature, Classification and Dimension of Cyber Crime

Chapter-4: Cyber Crime and Cyber Security: Indian Cases

Chapter-5: Socio-Economic Impact of Cyber Crime

Chapter-6: An evaluative study of legislative measures to control Cyber Crimes

Chapter-7: Concluding observations and to suggestions

Bibliography