CHAPTER 1

INTRODUCTION

Cyber Crime is a crime which involves the use of digital technologies in commission of offence, directed to computing and communication technologies. The modern techniques that are proliferating towards the use of internet activity results in creating exploitation, vulnerability making a suitable way for transferring confidential data to commit an offence through illegal activity. The activity involves like attacking on Information center Data System, theft, child pornography built images, online transaction fraud, internet sale fraud and also deployment in internet malicious activities such as virus, worm and third party abuse like phishing, email scams etc. The universal approach of network like internet at all levels of network needs to recover from committing illegal activity in all over the world and to stop the criminal nature by protecting unlawful activity by enforcing different level of firewall setting within its offline control for every nation in order to monitor and prevent crimes carried out in cyberspace. Network security controls are used to prevent the access of hackers in networks which includes firewall, virtual private networks and encryption algorithms. Out of these, the virtual private network plays a vital role in preventing hackers from accessing the networks. Virtual Private Network (VPN) provides end users with a way to privately access information on their network over a public network infrastructure such as the internet.

1.1 INFORMATION ON CYBER CRIME

In the beginning of certain development era, people were well motivated to attain a good progress in existing technological activities. Since the start of civilization period, the man has been always motivated by need to make better progress in the existing
technologies. According to the Department of Defense in America in 1969, the design of parallel super network known as ARPANET (Advanced Research Project Agency) was commissioned. It consisted of more than 50 computers that were connected with web links for the purpose of military operations. These networks steadily grew and then it was called online Internet activity for sharing business regime where communication was done in both modes Cyberspace.

Cyber law is a common term which refers to legal jurisdiction and other ways of preceding regulatory aspects in the internet. It is a constantly generic process. Whenever an internet development strategy follows, numerous amendments are enforced while it is developed, consequently numerous legal issues are also gets developed by illegal activists. In the Internet, Child Pornography is one of the serious Cybercrime and online pedophiles track to indulge children into sex activities using Internet. The traffic hazards, allotment in distributions, dissemination of obscene material, and posting includes pornography with all its filthy exposure constitutes the most important known criminal cyber offence today. This is one which threatens to challenge the development of technology of the younger creation in cybercrime and also leaving permanent scar and damage on the younger generation, if can’t restricted.

Cyber annoyance is a unique form of harassment in cybercrime. Various categories of harassment take place in cyberspace or with the use of cyberspace to attain criminal offence. Harassment can be sexual, religious, racial or other. People who involve perpetuating such harassment are guilty of cybercrimes. Cyber harassment brings us to another related offending area of violation of privacy of netizens. Another Cybercrime against persons is Cyber stalking. Harassments and Stalking are problems that many people especially like women face in their real life.

Another category of Cybercrimes is Cybercrime against property in diverse forms. These offences include unauthorized computer trespass through cyberspaces,
computer destruction, and broadcast of injurious programs and unofficial tenure of computerized data. Hacking and cracking are in the midst of the largest Cybercrimes known until this day. Hacking is entering a computer system without knowledge and consent of the authorized person, tampering with the precious and confidential data or information. Using one's own programming abilities and also various programmers with the intention to gain access to computer or network through unauthorized access are very serious crimes. Likewise, the dissemination and creation of harmful computer programs or other malicious virus which causes irreparable harm to computer systems is another category of Cybercrime and this Software piracy is also another distinct variety of Cybercrime. It is perpetuated by many people of cyber world for online who distributes unauthorized and illegal pirated copies of software products.

Another category of Cybercrime is against administration. Cyber Terrorism is a kind of crime which is distinct in this category. The increase of Internet has shown that the standard of Cyberspace is used by either group or individual to threaten the worldwide governments and to frighten the citizens of the country. This crime manifests when an individual "cracks" a government or military maintained website. The cyber crime may be broadly classified into three groups [21]. They are

1. Crime against the Individuals
   a. Person
   b. Property of an individual.

2. Crime against Organization
   a. Government
   b. Firm, Company and Group of Individuals.

3. Crime against Society

The following are the crimes that have been committed against the followings group:
AGAINST INDIVIDUALS

a. Harassment via electronic mails
b. Dissemination of obscene material.
c. Cyber-stalking.
d. Defamation.
e. Indecent exposure.
f. Cheating.
g. Unauthorized control/access over computer system.
h. Email spoofing.
i. Fraud.

AGAINST INDIVIDUAL PROPERTY

a. Computer vandalism
b. Transmitting virus.
c. Netrepass.
d. Unauthorized access / control over computer system

e. Intellectual Property crimes
f. Internet thefts

AGAINST ORGANIZATION

a. Unauthorized access / control over computer system.
b. Cyber terrorism against the government organization.
c. Possession of unauthorized information.
d. Distribution of Pirate software.

AGAINST SOCIETY

a. Child pornography
c. Indecent exposure of polluting the youth financial crimes.
d. Sale of illegal articles.
e. Trafficking.

f. Forgery.

g. Online gambling.

The Department of Justice for computer crime categorizes the use of computer in cyber crime into three ways as follows:

- The computer as a weapon - using a computer as a tool to commit "conventional crime" in the physical world (such as illegal gambling or fraud).
- The computer as a target - attacking the other computers (spreading viruses is an example).
- The computer as an accessory - using computer a "fancy file cabinet" used to store an ornament like illegal information.

1.2 HOW CYBER CRIMINALS WORK

Cyber crime has become a profession and the demography of the cyber criminal is changing rapidly with the type of organized gangsters who are more traditionally associated with drug-trafficking, extortion and money laundering. The question of how to obtain credit card/bank account data can be answered by a selection of methods each involving their own relative combinations of risk, expense and skill. The probable marketplace for this transaction is a hidden IRC (Internet Relay Chat) chat room.

Gaining control of a bank account is increasingly accomplished through phishing. All of the following phishing tools can be acquired very cheaply.

The cyber criminals works in the following ways:

**Coders**

They are the comparative veterans of the hacking community. With a few years' experience at the art and a list of established contacts, ‘coders’ produce ready-to-use tools (Trojans, mailers, custom bots) or services (such as making a binary code
undetectable to AV engines) to the cyber crime labour force – the ‘kids’. Coders can make a few hundred dollars for every criminal activity they engage in.

**Kids**

It is called so because of their tender age, most are under 18. They buy, trade and resell the elementary building blocks of effective cyber-scams such as spam lists, PHP mailers, proxies, credit card numbers, hacked hosts, scam pages etc. ‘Kids’ will make less than $100 a month, largely because of the frequency of being ‘ripped off’ by one another.

**Drops**

These individuals convert the ‘virtual money’ obtained in cyber crime into real cash. Usually located in countries with lax e-crime laws (Bolivia, Indonesia and Malaysia are currently very popular), they represent ‘safe’ addresses for goods purchased with stolen financial details to be sent, or else ‘safe’ legitimate bank accounts for money to be transferred illegally, and paid out of legitimately.

**Mobs**

These are professionally operating criminal organization which combines all of the above covered functions. Organized crime makes particularly good use of safe ‘drops’, as well as recruiting accomplished ‘coders’ onto their payrolls.

### 1.3 TYPES OF CYBER HACKERS

**White hat hacker:**

A white hat hacker is an ethical hacker who ethically oppose to the abuse of computer systems. A white hat generally focuses on securing IT systems, whereas a black hat (the opposite) would like to break into them. The term white hat hacker is also often used to describe those who attempt to break into systems or networks in order to help the owners of the system by making them aware of security flaws, or to perform some other altruistic activity. Many such people are employed by computer
security companies; these professionals are sometimes called as sneakers. Groups of these people are often called as tiger teams.

**Black hat hackers:**

A black hat is a person who compromises the security of a computer system without the permission of authorized party, typically with malicious intent. The somewhat similar activity of defeating copy prevention devices in software which may or may not be legal in a country's laws is actually software cracking. The primary difference between white and black hat hackers is that a white hat hacker claims to observe ethical principles. Like black hats, white hats are often intimately familiar with the internal details of security systems, and can delve into obscure machine code when needed to find a solution to a tricky problem. Some use the term grey hat and fewer use brown hat to describe someone's activities that crosses between black and white.

**Grey Hat Hackers:**

A Grey Hat in the computer security community, refers to a skilled hacker who sometimes acts legally, sometimes in good will, and sometimes not. They are a hybrid between white and black hat hackers. They usually do not hack for personal gain or for malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits.

**Internet Crime Hackers:**

Internet crime hackers commit crime on the internet, using the Internet and by means of the Internet. Internet crime is a general term that includes crimes such as phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on. All such crimes are computer related and facilitate crimes. The different types of Internet crime vary in their design and easy accessibility to be committed. It can be separated into two different categories.
Blackmail Hackers:

Blackmail is a long-established illegal act that has been given a new twist in the modern age. The blackmailer may threaten to release embarrassing or other harmful information via the Internet or a private network if the victim does not comply with the demands of the criminal. A cybercrime of this type may go as far as having the victim transfer funds to an untraceable bank account using some type of online payment program, thus making full use of modern technology to commit the crime Blackmail Hackers hack

i) Official government websites.

ii) On line credit card scam

iii) Work on cyber crime operations and they make money.

1.4 TIPS TO GET PROTECTED FROM CYBER CRIME

Some easy tips to protect computers from the growing threats:

Terminate Online Session Completely:

Closing the browser window or typing in a new website address without logging out may give others a chance of gaining access to your account information. Always terminate your online session by clicking on the "Log out or Sign Out" button. Avoid using the option of "remember" your username and password information.

Create Backup of Important Data:

Backup of all the important files whether personal or professional should be created. Getting used to back up your files regularly is the first step towards security of your personal computer.

Use Security Programs:

If your system does not have data protection software to protect online, then by all means buy internet security program for your computer. Today, almost all new computer systems come with some kind of security programs installed.
**Protect Your Password:**

Try creating a password that consists of a combination of letters (both upper case and lower case), numbers and special characters. Password should be changed regularly. Do not share your password with other people.

**Participation in Social Networking:**

While participating in most social networking sites do not expose the personal information to others and all of these sites have a certain intensity of control over security issues. Use privacy settings to prevent personal information being broadcast.

**Use Your Own Computer:**

It's generally safer to access your financial accounts from your own computer only. If you use some others computer, always delete all the "Temporary Internet Files", and clear all your "History" after logging off your account.

**Update Your Software Package Regularly:**

Frequent online updates are needed for all the Internet security software installed on your computer system.

**Using Email:**

A simple rule in using this communication tool is not to open any links in emails from people you do not know. Hackers do use E-mail as the main target seeking to steal personal information, financial data, security codes and other. Do not use the link sent to you. If you need access to any website, visit the website by typing the address in your menu bar. Cyber crime, being a burning issue around the world, many countries is beginning to implement laws and other regulatory mechanisms in an attempt to minimize the incidence of cybercrime. The laws in many countries on effectiveness of the punishment and prevention of computer crime requires a robust number and scope of the regulations, and even the proceedings, which lags far behind the reality of demand for computer crime in judicial practice.
1.5 A SET OF RESEARCH QUESTIONS ALONG WITH HYPOTHESIS & METHODOLOGY

1. Whether the present method of approach of cyber security is sufficient for prevention of cyber crime? If not, specify what is needed to establish a strong security?

No. Since all the research papers dealing with the cyber security use the concept of firewall only.

Requirement needed to establish a strong security:

The latest network security device called as Manageable Router acts as a firewall and in which classifier technique is essentially implemented inside the firewall as a policy mechanism to safeguard the traffic from hacking of packets (Information).

2. Whether the intrusion detection mechanism is adopted in the present method of approach of Cyber security? If not, specify what is needed to establish a strong security?

No. Since all the research papers dealing with the cyber security used the concept of Antivirus mechanism.

Requirement needed to establish a strong security:

The latest approach of security called Malware Detection Mechanism is needed to ensure that an intruder is entered in the cyberspace. The various methods of intrusion detection mechanism are Clustering approach.

3. Whether the Information Technology (Amendment) Act, 2008 are enough to prevent the cyber crime?

No. Still there are some deficiencies as well as contradictions with other existing laws.

Drawbacks of the Information Technology (Amendment) Act 2008 are

A. Under section 69, Government official or policeman will be able to listen to all
Neitizen phone calls, read your SMSs and emails, and monitor the websites you visit. Also he will not require any warrant from a magistrate to do so. It appears to be in violation of Article 21 of the Constitution — “no person shall be deprived of his life or personal liberty except according to procedure established by law.” It is unfortunate that a democratic and independent India has passed a law which is far more detrimental to personal liberty.

B. Section 2(na) introduced to define the term "Cyber Cafe". A place where access to Internet is allowed to public is called "Cyber Cafe". Any other network where closed groups such as employees or students are allowed is not covered.

C. Sec 50 specifies qualifications for appointment of Chairperson and Members of the Cyber Appellate Tribunal. Choice of members is restricted to Government Officers. Other talent cyber consultants are not considered as a Member in the Cyber Appellate Tribunal.

4. Whether a Research Scholars doing research in Cyber crime can give suggestion to the future Amendment of Information Technology Act, 2008?

   Yes. Research Scholars can give suggestions easily for the future Amendment of Information Technology (Amendment) Act, like many cyber consultant and Supreme Court Advocates who are practicing in the area of Cyber laws.

5. Whether the current Cyber security methods follow all the security procedure to protect the network vulnerabilities?

   No, that is the reason for existing vulnerability in the network. This also helps the intruder to hack the networks easily.

6. What way “The prevention of Cyber Crime using various Laws and Security Methods is useful to Netizens, Advocates and Network Engineers?

   Prevention of Cyber Crime using various Laws and Security methods is the hybrid approach which connects the role of Network Engineers (Internet Security) as
well as Advocates (Information Technology and various laws Amendments).

Network Engineer needs knowledge about “Information Technology Act and its Amendments Act”. Similarly Advocates needs the knowledge of “Various security methods like Firewall and Intrusion Detection”. Netizens needs both the knowledge. This research work helps to satisfy all their needs.

7. Whether the outcome of the research work is possible to show the experimental research work in real environment?

Yes. Our experimental research work environment for Network Security is real environment only. Our research work part in Law is concerned, to give suggestions for Amendments of the existing Information Technology (Amendment) Act, 2008 as well as possible to give suggestion for the enactment of new law regarding the Information Technology.

8. Who are possible to utilize and implement the proposed research work “Prevention of Cyber crime using various Laws and security methods” in real world?

First, for real experimental results the Network Service Provider utilizes effectively the proposed method in his router, which will be useful to his all subscribers as well as all Netizens in the real world. Secondly the Parliament Act Enactment Committee utilizes the proposed research amendments which we will suggest at the end of my research work, which will be useful to all the Netizens as well as the public in real world.

1.6 MOTIVATION AND OBJECTIVE

The motivation of this research is that, there are many disturbing things happening in cyberspace. Cybercrime refers to all the activities done with criminal intent in cyberspace. These could either be the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the new medium. Because of the anonymous nature of the Internet, it is possible to engage into a variety of criminal
activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. However, any activities which basically offend human sensibilities can also be included in its ambit.

The objective of this research is the prevention of cyber crime using cyber laws and cyber security methods. The cyber security methods classifies accurately and efficiently detects suspicious URLs, detects malware samples and phishing websites using clustering techniques, the generation of security test to find web application vulnerabilities using balanced approach.

1.7 ORGANIZATION OF THE THESIS

This thesis is organized in the following manner.

Chapter 1 gives a broad overview of prevention of cyber crime using cyber laws and cyber security methods.

Chapter 2 gives a brief discussion of previous works in prevention of cyber crime using cyber laws and cyber security methods.

Chapter 3 discusses the Methodology for Prevention of Cyber Crime using Cyber Laws.

Chapter 4 deals with the Methodology for Prevention of Cyber Crime Using Classifier Accurately and Efficiently Detects Suspicious URLs.

Chapter 5 explains the Methodology for Prevention of Cyber Crime Using Detecting Malware Samples and Phishing Websites Based on Clustering Techniques.

Chapter 6 deals with the Methodology for Prevention of Cyber Crime Using Generation of Security Test to Find Web Application Vulnerabilities Based on Balanced Approach.

Chapter 7 deals with the Recommendations and Suggestions of the Prevention of Cyber Crime.
Chapter 8 concludes with the research findings and enumerates the future enhancements.