International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015
ISSN 2091-2730

Cyber Crime: A Changing Threat Scenario in the State Of Art

Raksha Chouhan

Faculty, Prestige Institute of Management and Research, Indore (Madhya Pradesh)
E-mail: raksha_chauhan@pimrindore.ac.in

The global cyber crime landscape has changed dramatically with criminals utilizing more sophisticated technology and greater knowledge of cyber security. Illegal profits have reached to amazing figures and it has become a business opportunity open to everybody driven by profit and personal gains. The alertness level towards cybercrime threats has increased and law enforcement acts globally to battle with them but Growing danger from crimes committed against electronic information on computers is alerting us to claim attention and developments towards cyber crime in the changing threat scenario has become demand of the state of art. In this research paper an analytical approach has been introduced to various trends used for cyber crime in the changing threat scenario. This paper also sheds light on different methods by which cyber crime is committed, who and why commits cyber crime?

Keywords: Cyber Attacks, Cyber Crimes, Cyber Law, I.T. Act 2000, I.T. Act 2008, National Security.

1. Introduction

In the present scenario advent of technological revolution has given broader opportunities and scope to internet users but at the same time this has led to the global high-tech cyber crime. Information technology (IT) has exposed the user to a huge data bank of information regarding everything and anything. However, it has also added a new dimension to terrorism. Recent reports suggest that the terrorist is also getting equipped to utilize cyber space to carryout terrorist attacks. The possibility of such attacks in future cannot be denied. Terrorism related to cyber is popularly known as 'cyber terrorism' [6]. Cybercrime deals with the crimes related to computer world. Since couple of decades India has imparted information technology in almost all the areas, mainly in Indian banking industry and financial institutions with its full optimization. India is rated in the top 5 countries affected with cyber crimes and gaining momentum from simple email type of crime to serious crime like hacking, phishing, Vishing, source code theft, cyber staking, internet time theft, Web Jacking and cross site scripting etc[1]. Thus cybercriminals have become more organized and adaptive, and continue to develop fraud-as-a-service models which make some of the most innovative and advanced threat and fraud technologies available to a much wider user base [16]. Etter in 2001 defines, "Offences where a computer is used as a tool in the commission of an offence, or as a target of an offence, or used as a storage device in the commission of an offence". According to Graham in 2001 Cyber fraud can be defined as: "A fraudulent behaviour connected with computerization by which someone intends to gain dishonest advantage". Smith in 2001 defines e-fraud as "any dishonest activity that involves the Internet as the target or means of obtaining some financial reward". Using the Graham's definition as a basis, e-fraud can be defined as the intersection of Cyber crime and Fraud as shown below [17]:

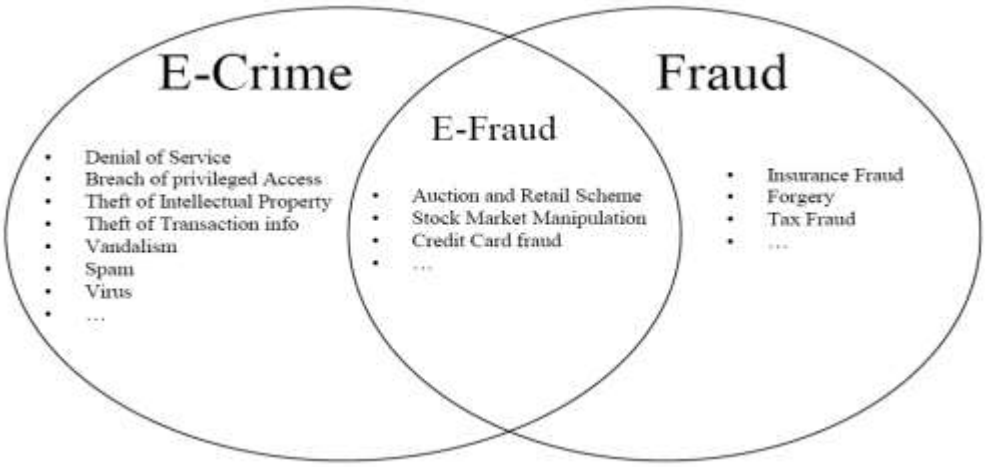

Fig 1: E-Fraud As an intersection of E-crime and fraud

Top modes of attack are Phishing attacks of online banking accounts, Cloning debit cards, e-mail frauds and Obscene publication etc. following figure shows status of global internet attacks in the year 2014 [11].

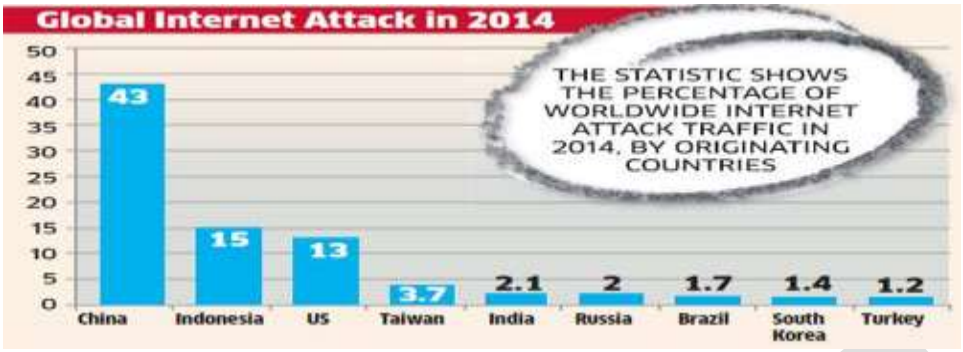

Fig 2: Status of Global Internet Attacks In the Year 2014

The following map demonstrates the top five countries ranked by the number of victim complaints reported to the IC3 during 2013 [9]:

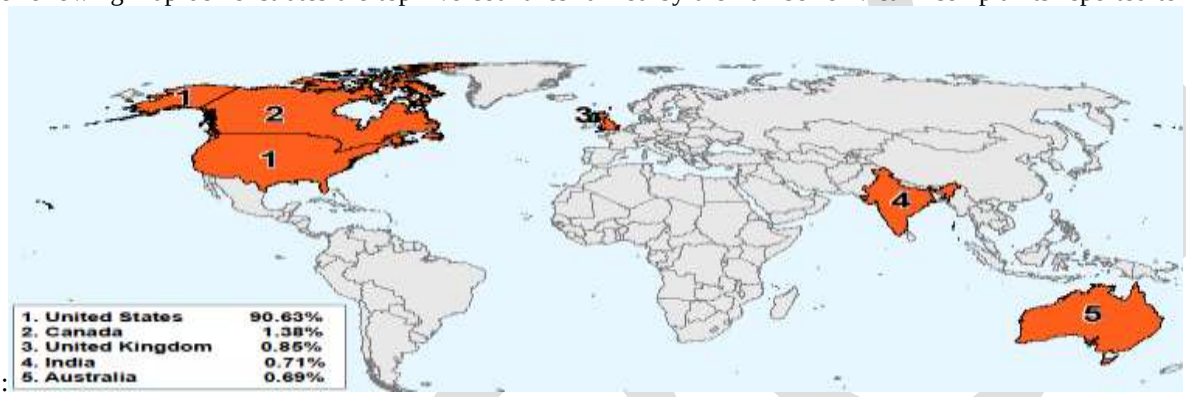

Fig 3: Rank of Top Five Countries According to the Number of Victim Complaints In 2013

2. Literature Review

Cybercrime is an activity performed by criminal by using an element of a computer or network of computers. In Cybercrime most radical changes can be seen in criminal behavior and it had a reflective impact on our lives in such a short space of time. Reports suggest that cyber attacks are understandably directed toward economic and financial institutions. Given the increasing dependency of the Indian economic and financial institutions on IT, a cyber attack against them might lead to an irreparable collapse of our economic structures. And the most frightening thought is the ineffectiveness of reciprocal arrangements or the absence of alternatives [6].

Methods of attack are becoming even more sophisticated with the passage of time. Online banking has existed since the 1980s [4]. In pre 2000 cybercrime was considered as immature or childish behavior of criminal as a practical joke or game by those who committed it. Earlier it was centered on or around one-man operated crime with the intension to exploit the limitations in the computer operating system or computer network. In most cases these crimes were committed by those people who felt challenged to prove that they could beat the system without any intension of gaining financial benefit where a great deal of financial damage could actually result. At this time Criminal defense policies was also largely based on the fact that no real intentional damage was done and, in a large number of cases, the penalty for the crime was showing how the computer system had been hacked by the hacker. In post 2000 cyber criminal gangs had introduced a professional element into the world of cybercrime. They had organized and focused their attention towards profit gain and had developed tactics to making use of computer networks to infiltrate and take advantage of the trust of other users of that computer network for huge financial gain. They had worked out hardened and they had realized that the Internet was a safe domain, with much less risk, with which to operate and generate large profits [3]. Few cases of fraud have been reported until 2004. That means that the escalation of attacks is relatively recent, and was concentrated in the last decade [4]. Fig 4 is showing various stages of cyber attack evolution from year 1980 to the year 2000+ [2]:

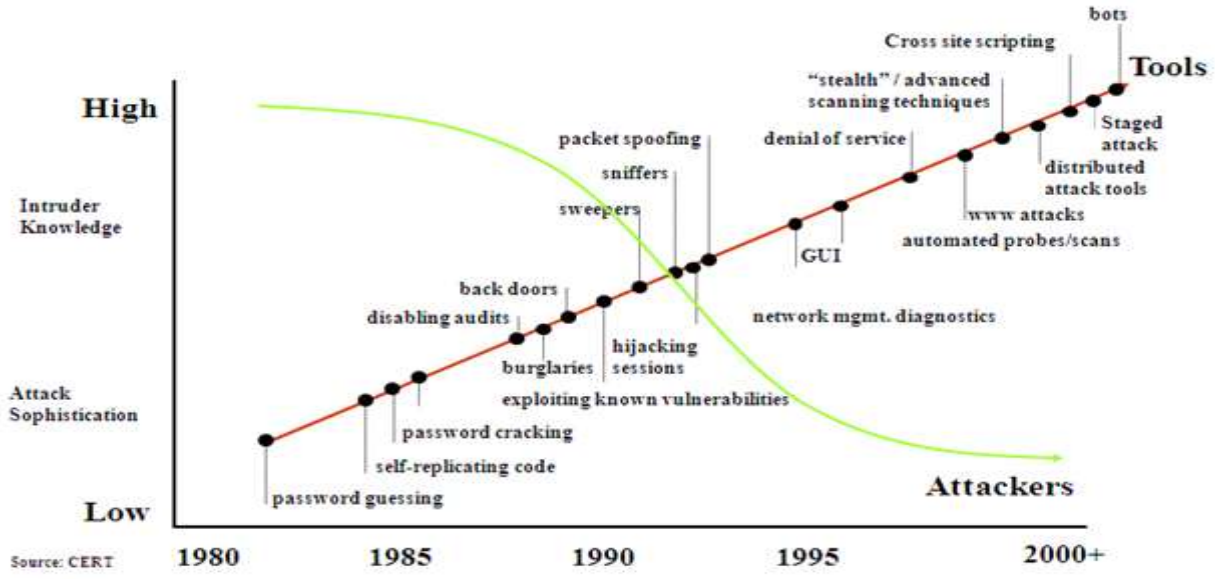

Fig 4: Various stages of cyber attack evolution

3. Objectives of the Study

1. To identify different methods by which cyber is committed? Who commits and reason behind why do people commit cyber crime?
2. How many cyber crimes are committed and what are the trends in the changing threat scenario.
3. To find out different methods by different point of view like legal, technical and strategic perspective to reduce cyber crime.

4. Methodology

This study is descriptive in nature. An attempt has been made to analyze cyber crime report given by different media resources from theoretical and investigative points of views with sentencing research. The material has been referred from Online as well as desk based book reviews, articles, reports, research and conference papers. Thus a combination of existing literature studies and in-depth secondary database material is used to fulfill the objective.

5. Methods and Taxonomy of Cyber Attacks

The most popular weapon in cyber terrorism is the use of computer viruses and worms. That is why in some cases of cyber terrorism is also called 'computer terrorism'. The attacks or methods on the computer infrastructure can be classified into three different methods that is **physical attack** in which the computer infrastructure is damaged by using conventional methods like bombs, fire etc., then **Syntactic Attacks** in which the computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictable. Computer viruses and Trojans are used in this type of attack and third method is **Semantic Attacks** which is more treacherous as it exploits the confidence of the user in the system. During the attack the information keyed in the system during entering and exiting the system is modified without the user's knowledge in order to induce errors [6]. In the following table taxonomy of cyber attacks has been shown [1] [7] [8]:

S. No.	Categories with Examples
1	**User based / against a Persons** i. Defamation/ Insult ii. SMS spoofing / Email spoofing/ Harassment Via Emails iii. Hacking/Unauthorized access iv. Offensive content exposure & harassment v. Cyber stalking / physical threat using computer technology vi. Broadcasting of prohibited materials / child Pornography vii. Trafficking in drug or human beings etc

	viii. Cheating & fraud like stealing password & data, ATM like credit/debit card fraud.
2	**Property based cyber crimes** i. EFT crime ii. Online theft iii. Computer vandalism. iv. Unauthorized access v. Virus Transmitting vi. Intellectual property vii. Offensive material Propagation viii. Electronic Money laundering and Tax avoidance ix. Hacking in terms of reputation loss of particular person or a company x. Cyber squatting in terms of registering, selling or using a domain name with the intent of profiting from the goodwill of someone else's trademark like www.yahoo.com and www.yaahoo.com.
3	**Society based cyber crime** i. Sale of illegal articles. ii. Forgery crimes like by fake threatening mails to mislead large number of people iii. Financial Crimes like use of debit/credit card by obtaining illegal password. iv. Child pornography like indecent exposure and obscenity. v. Trafficking in drugs/arms weapons/human beings etc vi. Online gambling like offering jobs, contractual crimes etc.
4.	**Private Organizations based** i. Theft of telecommunications services. ii. Telecommunications Piracy iii. Unauthorized control/access over computer system iv. Ownership of non-permitted information. v. Distribution of pirated software etc.
5	**Government based cyber crime** i. Distribution of pirated software ii. Ownership of Unauthorized Information iii. Cyber welfare refers to politically motivated hacking. iv. Cyber Terrorism like DDoS, sensitive computer network, denial of services, v. Defacement of websites etc.

Table 1: Cyber Crime Taxonomy

6. Advantages on online criminality/Fraud against traditional crime (why criminal commits cyber crime)

Cyber crimes are reasonably easy with low risk and hard to trace because:
1. Low amount of time, effort and money is required.
2. Secrecy is maintained without Physical presence.
3. Encryption is much better than a good concealing outfit.
4. Evidence of a crime can be easily wiped out.
5. Ethical limitations are very few.
6. No eyewitnesses.
7. Massive audience target with unlimited geographical coverage
8. Easy to mislead victims online cover their tracks by using aliases and unknown re-mailers.
9. Majority of victims don't file complaints and as a result fraudster motivates towards another fraud.

7. Role playing factors responsible for cyber crime

The integrity, authenticity, confidentiality and availability of data in cyberspace have become vital questions of the 21st century. The trends of Information Systems such as Internet and cloud computing has created challenges in maintaining security of information. Data interception, data modification, data theft, network crime, access crime etc are the fundamental categories of cyber crimes. **A**ccountable factors which are responsible for cyber crime are-

1. Data access and sharing policies between private and public sectors.
2. Data leakage through mobile and wireless frauds and cloud computing also plays important role to augmentation of cyber crime.
3. Criminals Justice sanctions like internet restrictions and electronic monitoring.

4. Sentencing of cyber criminals etc.

8. Cyber Crime Trends in Current Scenario

India has emerged as a favourite among cybercriminals, mostly hackers and other malicious users who use the internet to commit crimes. According to an Assoc ham-Mahindra SSG study "The number of cyber crimes in the country may double to 3 lakh in 2015 and could pose serious economic and national security challenges". The increasing use of smart phones and tablets for online banking and other financial transactions have increased risks. Phishing attacks of online banking accounts or cloning of ATM/debit cards are common occurrences. The attacks have mostly originated from the cyber space of countries including the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria and the UAE, the study revealed. Smartphone users rarely check for security certificates while downloading apps (games, music and other software) from third party or unsecured sites, the study said, adding that mobile banking apps store data such as PIN and account number, on the phone. It further stated that mobile frauds are an area of concern for companies as 35-40 per cent of financial transactions are done via mobile devices and this number is expected to grow to 55-60 per cent by 2015 [10]. According to Computer Emergency Response Team-India (CERT-In) report till may 2014 total 9,9,174 Indian websites were hacked by hacker groups spread across the world [13].

The true volume and scope of cyber crime is indefinite and criminals continue to use a variety of scams to defraud Internet users. FBI IC3 (Federal Bureau of Investigation International Crime Complaint Center) receives wide variety of complaints on a different crime schemes from simple frauds to complex hacking and malicious software or malware scams. In 2013, the IC3 received 262,813 consumer complaints with an adjusted dollar loss of $781,841,6111, which is a 48.8 percent increase in reported losses since 2012 ($581,441,110). Of the 262,813 complaints received in 2013, 45.5 percent (119,457) reported financial loss. Year wise complaints registered in IC3 has been shown below [9]-

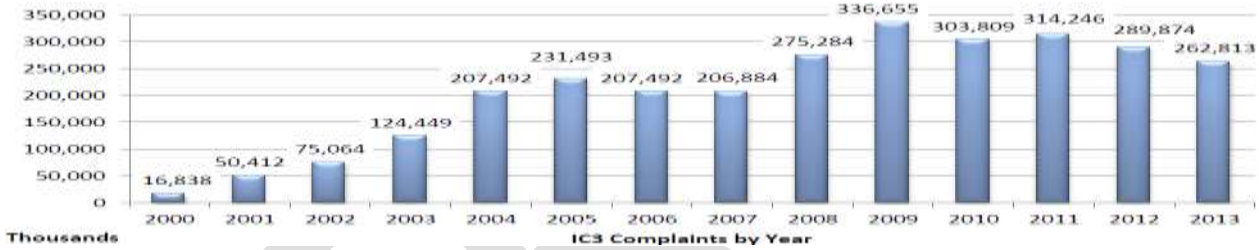

Fig 5: Year wise Status of IC3 complaints against cyber crime

Indian cyber law is still ineffective in delivering cyber crime convictions, even as cyber fraud continues to increase. The year 2013 has seen a lot of events as far as cyber law jurisprudence in India are concerned. It has been an eventful year that demonstrated how cyber legal challenges are increasingly becoming relevant. According to the information reported to and tracked by Indian Computer Response Team (CERT-In), a total number of 308,371 websites of which 78 belonged to government were hacked between 2011 and 2013 (up to June). Hackers of the Pakistan Cyber Army (PCA) breached and defaced seven websites owned by the Indian government. The year 2013 has also seen the increase in the use of power of blocking for the purposes of blocking various websites. Internet Service Providers blocked torrent websites, like The PirateBay and some others like, Vimeo. Some sites were blocked on judicial orders. Government of India has been quietly working in the year 2013 on a new legislation on privacy that can provide India a substantial basis for protection and preservation of privacy, both personal and data privacy [12].

In the following table Cyber Crimes/Cases registered and Persons Arrested under IT Act during 2010-2013 has been given in decreasing order [14]:

SL. No.	Crime heads	Cases Registered				% Variation in 2013 over 2012	Persons Arrested				% Variation in 2013 over 2012
		2010	2011	2012	2013		2010	2011	2012	2013	
1	Tampering computer source documents	64	94	161	137	-14.9	79	66	104	59	-43.3
2	Hacking with computer system										
	i) Loss/damage to computer resource/utility	346	826	1,440	1,966	36.5	233	487	612	818	33.7
	ii)Hacking	164	157	435	550	26.4	61	65	137	193	40.9
3	Obscene publication/transmission in electronic form	328	496	589	1203	104.2	361	443	497	737	48.3
4	Failure										
	i) Of compliance/orders of certifying authority	2	6	6	13	116.7	5	4	4	3	-25.0
	ii) To assist in decrypting the information intercepted by govt. agency	0	3	3	6	100.0	0	0	3	7	133.3
5	Un-authorised access/attempt to access to protected computer system	3	6	3	27	800.0	6	15	1	17	1600.0
6	Obtaining licence or digital signature certificate by misrepresentation/suppression of fact	9	6	6	12	100.0	4	0	5	14	180.0
7	Publishing false digital signature certificate	2	3	1	4	300.0	2	1	0	8	@
8	Fraud digital signature certificate	3	12	10	71	610.0	4	8	3	51	1600.0
9	Breach of confidentiality/privacy	15	26	46	93	102.2	27	27	22	30	36.4
10	Other	30	157	176	274	55.7	17	68	134	161	20.1
	Total	966	1,791	2,876	4,356	51.5	799	1,184	1,522	2,098	37.8

Note- @indicates infinite percentage variation because of division by zero

Table 2: Cyber Crimes/Cases registered and Persons Arrested Under IT Act During 2012 & 2013 with Percentage of Variation.

In the following table Incidence of Cases Registered under Cyber Crimes in various States During 2012 & 2013 and Percentage of Variation has been given in decreasing order [14]:

S. No.	Name of the State	IT Act			IPC Section		
		2012	2013	% of variation	2012	2013	% of variation
1	MAHARASHTRA	471	681	44.6	90	226	151.1
2	ANDHRA PRADESH	429	635	48.0	25	16	-36.0
3	KARNATAKA	412	513	24.5	25	20	-20.0
4	UTTAR PRADESH	205	372	81.5	44	310	604.5
5	KERALA	269	349	29.7	43	34	-20.9
6	MADHYA PRADESH	142	282	98.6	55	60	9.1
7	RAJASTHAN	147	239	62.6	7	58	728.6
8	WEST BENGAL	196	210	7.1	113	132	16.8
9	PUNJAB	72	146	102.8	6	10	66.7
10	HARYANA	66	112	69.7	116	211	81.9

Table 3: Incidence of Cases Registered under Cyber Crimes in various States during 2012 & 2013

Cyber crimes – cases of various categories under IT Act, 2000- As it is clear from table 2 that total 4,356 cases were registered under IT Act during the year 2013 and 2,876 cases were registered in the previous year (2012), thus showing an increase of 51.5% in 2013 as compare to 2012. As it is clear from table 3 that 15.6% of total such cases (681 out of 4,356 cases) were reported from Maharashtra followed by Andhra Pradesh (635 cases), Karnataka (513 cases), Uttar Pradesh (372cases), Kerala (349 cases), Madhya Pradesh (282 cases), Rajasthan (239 cases), West Bengal (210 cases), Punjab (146 cases) and Haryana (112 cases).

In the Following table Incidence of Cases Registered and Number of Persons Arrested under Cyber Crimes (IT Act) during 2013 at All-India level has been shown:

Sl. No	Crime Head	Cases Registered	Persons Arrested
(1)	(2)	(3)	(4)
	A. Offences under IT Act		
1	Tampering computer source documents	137	59
2	Hacking with Computer Systems		
	i) Loss/damage to computer resource/utility	1966	816
	ii) Hacking	550	193
3	Obscene publication/transmission in electronic form	1203	737
4	Failure		
	i) Of compliance/orders of certifying Authority	13	5
	ii) To assist in decrypting the information intercepted by Govt. Agency	6	7
5	Un-authorised access/attempt to access of protected Computer system	27	17
6	Obtaining License or Digital Signature Certificate by misrepresentation/suppression of fact	12	14
7	Publishing false digital Signature Certificate	4	2
8	Fraud Digital Signature Certificate	71	51
9	Breach of confidentiality/privacy	93	30
10	Other	274	161
12	Total (A)	4356	2098

Table 4: Cases Registered and Number of Persons Arrested Under IT Act In 2013

In the Following table Incidence of Cases Registered and Number of Persons Arrested under Cyber Crimes (IPC section) during 2013 at All-India level has been shown:

Sl. No	Crime Head	Cases Registered	Persons Arrested
(1)	(2)	(3)	(4)
	B. Offences under IPC		
1	Offences by/Against Public Servant	1	2
2	False electronic evidence	6	7
3	Destruction of electronic evidence	6	4
4	Forgery	747	626
5	Criminal Breach of Trust/Fraud	518	471
6	Counterfeiting		
	i) Property/mark	10	34
	ii) Tampering	8	10
	iii)Currency/Stamps	41	49
7	Total(B)	1337	1203

Table 5: Cases Registered and Number of Persons Arrested Under IPC section in 2013

As it is clear from the table 4 that under cyber crime IT Act out of 4356 registered cases only 2098 persons were arrested, i. e. only 48.16% persons were arrested and 51.84% persons were not arrested and in the table 5 under IPC Section out of 1337 registered cases only 1203 persons were arrested, i. e. total 89.97% persons were arrested and only 10.03% persons were not arrested. Thus under IT Act more cases were registered as compare to IPC Section but the percentage of persons arrested in IPC section is more than the persons arrested in IT Act. **Overall** 5693 (4356+1337) cases were registered under IT Act and IPC Sections and only 3301 (2098+1203) persons were arrested under IT Act and IPC Section i. e. total 57.98% persons were arrested under both the categories and 42.02% were left as it is. These figures show unawareness and needs strong standards and regulations at strategic and legal perspectives.

In the Following table Persons Arrested under Cyber Crimes (IT Act) By Age Group During 2013 at All-India level has been shown:

Sl. No	Crime Head	Below 18 Years	Between 18 – 30 Years	Between 30 –45 Years	Between 45 – 60 Years	Above 60 Years	Total (All Age Groups)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	A. Offences under IT Act						
1	Tampering computer source documents	1	23	24	11	0	59
2	Hacking with Computer Systems						
	i) Loss/damage to computer resource/utility	10	454	307	44	3	818
	ii) Hacking	2	92	91	6	2	193
3	Obscene publication/transmission in electronic form	20	457	203	53	4	737
4	Failure						
	i) Of compliance/orders of certifying Authority	0	1	2	0	0	3
	ii) To assist in decrypting the information intercepted by Govt. Agency	3	4	0	0	0	7
5	Un-authorised access/attempt to access of protected Computer system	0	9	8	0	0	17
6	Obtaining License or Digital Signature Certificate by misrepresentation/suppression of fact	0	10	4	0	0	14
7	Publishing false digital Signature Certificate	0	4	3	1	0	8
8	Fraud Digital Signature Certificate	0	27	19	5	0	51
9	Breach of confidentiality/privacy	0	19	8	3	0	30
10	Other	9	90	53	8	1	161
11	Total (A)	45	1190	722	131	10	2098

In the Following table Persons Arrested under Cyber Crimes **(IPC Sections)** By Age Group During 2013 at All-India level has been shown:

Sl. No	Crime Head	Below 18 Years	Between 18 – 30 Years	Between 30 –45 Years	Between 45 – 60 Years	Above 60 Years	Total (All Age Groups)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	B. Offences under IPC						
1	Offences by/Against Public Servant	0	2	0	0	0	2
2	False electronic evidence	0	6	0	1	0	7
3	Destruction of electronic evidence	0	3	1	0	0	4
4	Forgery	0	263	305	54	4	626
5	Criminal Breach of Trust/Fraud	0	145	260	66	0	471
6	Counterfeiting						
	i) Property/mark	0	8	15	9	2	34
	ii) Tampering	0	2	3	5	0	10
	iii)Currency/Stamps	0	19	19	9	2	49
7	**Total(B)**	**0**	**448**	**603**	**144**	**8**	**1203**

Table 7: Persons Arrested Under Cyber Crimes (IPC Sections) By Age Group In 2013

As shown in table 6 Under IT Act total 2098 persons were arrested from all age groups wherein 1190 persons were between age group 18-30 years and 722 persons were from the age group 30-45 years. Similarly in the table 7 under IPC Section total 1203 persons were arrested from all age groups wherein 603 from age group 30-45 and 448 from age group 18-30. **Thus** under IT Act cyber crime percentage of age group 18-30 is more whereas Under IPC Section Cyber crime percentage of age group 30-45 is more.

It can be concluded that under IT Act for the cyber crime like hacking, obscene publications, unauthorized access, digital signature certificate fraud and violation of confidentiality, persons of age group 18-30 are more involved **whereas** under IPC Section offences like forgery, criminal violation of trust and counterfeiting, persons of age group 30-45 are more involved.

Federal Investigative Law Enforcement and Regulatory Agencies

For the determination of some of the federal investigative law enforcement agencies that may be appropriate for reporting certain kinds of crime, following table can be referred [15].

Type of Crime	Appropriate federal investigative law enforcement agencies
Computer intrusion (i.e. hacking)	• FBI local office • U.S. Secret Service • Internet Crime Complaint Center
Password trafficking	• FBI local office • U.S. Secret Service • Internet Crime Complaint Center
Counterfeiting of currency	• U.S. Secret Service
Child Pornography or Exploitation	• FBI local office • if imported, U.S. Immigration and Customs Enforcement • Internet Crime Complaint Center
Internet fraud and SPAM	• FBI local office • U.S. Secret Service • Federal Trade Commission (online complaint) • if securities fraud or investment-related SPAM e-mails, Securities and Exchange Commission (online complaint) • Internet Crime Complaint Center
Internet harassment	• FBI local office
Internet bomb threats	• FBI local office • ATF local office

Table 8: Federal Investigative Law Enforcement Agencies

9. Conclusion and Suggestions

Rising Internet penetration and online banking have made India a favourite among cybercriminals, who target online financial transactions using malicious software (malware). According to the studies done in 2014 after Japan and US, India has ranked third in the list of countries most affected by online banking. In case of revenue generation Andhra Pradesh, Karnataka and Maharashtra together contribute more than 70 per cent to India's revenue from IT and IT related industries [10]. The pace at which cybercrime is emerging is one of the most alarming trends. In recent years, cyber crime has grown by leaps and bounds. Cyber crime revenue grew to levels comparable to that of a state, and major security analysts agree that it will experience sustained growth in the coming years. The improvement of online banking system and its increased use by consumers worldwide has made this service a privileged target for cyber criminals [4]. Phil Williams, a visiting scientist at CERT, summarize the issue concisely. "The Internet provides both channels and targets for crime and enables them to be exploited for considerable gain with a very low level of risk For organized crime it is difficult to ask for more" [5].

Cyber attacks have come not only from terrorists but also from neighboring countries unfavorable to our National interests. Small business generally faces online fraud risks as well as unaware people who responds to consumer scam invitations. Threat of cybercrime is coming out on intense level towards the economy, peace and security of our nation hence a holistic approach is required to fight with present scenario to provide ensured security in all consequences. There is no one measure that will cure the danger of cybercrime and ensure cyber security and due to complex nature of cybercrime it has become difficult to battle with it. It is necessary for individuals, organizations and government to take initiatives like to educate and create awareness on security practices by addressing people, process and technology issues as well as regarding to the collection of digital forensics evidences; and how to report cybercrime. In the following table suggestions from various perspectives has been discussed:

S. No.	Categories of Perceptions	Suggestions
1.	**Technical perspective**	1. Net security should be increased. 2. DTS (Digital Time Stamping System) should be used. 3. Encryption technology should be used for processing, storage and transfer of data. 4. Mails or applications sent from unknown sources or not signed should be ignored. 5. Status of device visibility should be hidden for Bluetooth mobile services. 6. Software's downloaded from internet should not be executed without scanning. 7. Compromised computers should be isolated from further threats spreading. 8. Filter software and voice recognizer should be used against unauthorized access. 9. Email server should be blocked or email should be removed for the files attachment with the extension .vbs, .bat, .exe, .pif and .scr to protect from threat spreading.

		10. Many Operating systems, by default install auxiliary services that are not critical. These services increase possibilities of attack. Installation of these services should be avoided. 11. Access control should be limited and password protection should be provided in case of file sharing. 12. Complex password protection should be given by user and updated ant-hijacking software's like anti-spyware, firewalls, IDS and IPS should be used. 13. High biometric/ forensic techniques should be involved as cyber security mechanism.
2.	**Legal Perspective**	1. False Email id registration should be treated as an offense. 2. Licenses of ISP should be reviewed periodically. 3. Appropriate changes according to recent threat scenario should be done to make the laws more effective well as enactment of new laws is required. 4. Cyber law should be universalized and universal legal regulatory mechanism should be adopted. 5. Establishment of special cyber court and investigation cell for high technology based crimes. 6. Standard regulations should be implemented towards uses of social networking sides. 7. Implementation of E-Judiciary and video-conferencing concept for speedy justice. 8. High penalties should be enforced for the committed cybercrime and for those who do not report the incident of cybercrime.
3.	**Strategic Perspective**	1. More investment in this field in terms of finance and manpower is required. 2. Organizations who are dealing with Cyber security should be given all support. 3. Joint efforts are required by all Government agencies including defence forces to attract qualified skilled personnel for implementation of counter measures. 4. There should be a cryptogrammic relationship between the Internet Service Providers, government and civil society so that legal framework towards cyber-security can become stronger. 5. Agreements relating to cyber security should be given the same importance as other conventional agreements. 6. A national cyber security technology frame-work should be developed to specify cyber security requirement controls and baseline for individual network user. 7. Current scenario needs to sensitize the common citizens about the dangers of cyber terrorism. National culture of security standards should be introduced and promoted. 8. Multifactor authentication with unique personal id like biometric identification, smart card etc can be included. 9. Cyber Crime awareness and education programs should be introduced and education system curriculum should be reviewed and proper training should be incorporated related with information and cyber security at all levels of education i. e. at primary and secondary level also.

Table 10: Recommendation to ensure cyber security

REFERENCES:

1. Raksha Chouhan, Shashikant Pardeshi (2013) "Cyber Crime Security and Upcoming Challenges: An Overview", Journal of Engineering, Science And Management Education (JESME), Quarterly Research Journal of NITTTR Bhopal, Vol-6, Issue-III, July–September 2013, PP 131-136, ISSN 0976-0121.
2. Lance James CTO, (July 2005), "Phishing an evolution", company confidential, secure science corporation Secure Science Corporation 7770 Regents Rd., Suite 113-535, San Diego, CA. 92122-1967, (877)570-0455, http://www.securescience.net.
3. Criminal Defense (visited: 8-1-15) "The evolution of cybercrime from past to the present" http://www.criminallawyergroup.com/criminal-defense/the-evolution-of-cybercrime-from-past-to-the-present.php.
4. Pierluigi Paganini, (November 5th, 2013), "Modern Online Banking Cyber Crime" http://resources.infosecinstitute.com/modern-online-banking-cyber-crime/.
5. Sumanjit Das and Tapaswini Nayak (October 2013), "Impact of cyber crime: issues and challenges", International Journal of Engineering Sciences & Emerging Technologies, ISSN: 22316604 Volume 6, Issue 2, pp: 142-153 ©IJESET.
6. Col S S Raghav (visited: 28-11-14), "cyber security in india's counter terrorism strategy", pp 5, ids.nic.in.
7. Dhawesh Pahuja (July 17, 2011) "Cyber Crimes And The Law", http://www.legalIndia.in/author/advocatedcpyahoo-com/, Legal Articles.

8. Calling off Cyber Crime>>Main Types of Cyber crime (visited: 8-1-15), https://sites.google.com/site/callingoffcybercrime/types-of-cyber-crime.
9. FBI IC3 (Federal Bureau of Investigation International Crime Complaint Center 2013) "2013 Internet Crime Report", visited on 10-1-15.
10. The Economic Times (Jan 5, 2015) "Cyber crimes in India likely to double to 3 lakh in 2015:Report",http://articles.economictimes.indiatimes.com/2015-01-05/news/57705670_1_cyber-crimes-online-banking-pin-and-account-number.
11. The Economic Times (09 Jan 2015) "A close look at the growing trend of cyber crimes in India". http://economictimes.indiatimes.com/tech/internet/A-close- look-at-the-growing-trend-of-cyber-crimes-in-India/articleshow/45815348.cms
12. Pavan Duggal (December 30, 2013)**"**The face of Indian cyber law in 2013", http://www.business-standard.com/article/technology/the-face-of-indian-cyber-law-in-2013-113123000441_1.html.
13. Computer Emergency Response Team-India (CERT-In) reports 62,189 cyber attacks till May 2014, http://www.techmistory.com/2014/07/cert-in-reports-62189-cyber-attacks.html, visited: 10-1-15.
14. National Cyber Crime Bureau Report (2013) "Crime in India-2013", http://ncrb.gov.in/, pp 6, visited:10-1-15.
15. Elham Fariborzi , Mahnaz Hajibaba (2012), "Computer crimes, problems, Law enforcement for solving complaints and education", 2012 International Conference on Education Technology and Computer (ICETC2012), IPCSIT vol.43, IACSIT Press, Singapore, pp 5.
16. White Paper, The Current State of Cybercrime 2014: An Inside look at the Changing Threat Landscape, EMC2 RSA report, downloaded on 3-nov-14, pp 9, www.emc.com/rsa.
17. Dr Hugh McDermott (visited: 24-1-15), Cyber Crime – Present and Future Trends Director, AML-CTF, Fraud & Financial Crime Program, Australian Graduate School of Policing, Charles Strut University, pp 52.