Cyber Crimes and Crime Registration in Indian Context – A Critical Analysis

Mr. Prasanna S[1] Dr. V. Mariappan[2]
[1]Research Scholar, Department of Banking Technology, School of Management, Pondicherry University
[2]Professor, Department of Banking Technology, School of Management, Pondicherry University

Abstract**:** Cyber crimes are crimes that happen in the electronic environment known as cyberspace. Cyber crimes are either directed at computer or electronic devices where computers/electronics devices are integral to such offense. The current paper attempts to map the trends and developments in the cyber crime scenario with reference to Indian context.

Keywords: Cyber Crime, Technology, Computer as a Tool and Target for Crimes

1. Introduction

Technological advancement has brought lots of convenience to individuals and business community. One such technology that has created a huge impact is internet. For individual it has changed the way they live, the way they communicate and the way they transact and for organization and business it saves time, cost and efforts in reaching their clients and satisfy their demands profitably. Even though internet has lot of benefits attached to it on the brighter side, it carries also security concerns in form of cyber crimes on the darker side.

Cyber crime is an illegal behavior that targets the security of computer systems and/or the data accessed and processed by computer networks. In simple it a criminal act that involve computer or internet in which computer is either a tool or target for the crime. The Computer Emergency Response Team India (CERT-In), the national level nodal agency for dealing with computer security incidents along with similar global agencies and Cyber Security Cells of State police departments, private and public sector institutions takes care of cyber security issues in India. The current paper attempts to map the trends and developments in the cyber crime scenario in India.

2. Growth of ICT and Its Impact

Introduction of smart phones, Internet and its penetration rate play a crucial role in the success of information and communication technology. According to the data released by ITU for the year 2016, developed countries has high internet penetration rate of 81 percent followed by developing and least developed countries with 40 and 15 percent respectively [1]. Out of One billion households that have internet access china tops the list with 230 million subscribers followed by India with 60 million subscribers. Besides this development of smart phones and its associated technology such as LTE have increased the internet usage and expected to have same impact in near future [1]. As per the global mobile market report the smart phone penetration in India is at 27.7 percent for the year 2018 which has increased from 22.4 percent of the previous year 2017 [2].

The information and communication technology has impacted different fields of society via business, education, science, medicine and health care, etc. Advancement in ICT has not only transformed the way the individuals and organization conduct business but also brought dramatic changes in the way they perform day to day activities. Integration of ICT in the organization function has increased productivity and efficiency which is evident from the results of the studies. Advancement in ICT has positively impacted individuals in personal and work life via psychological well being, flexible work hours and improved ability in doing task.

3. User Awareness Regarding Cyber Crime

In today’s environment computer and electronic communication devices are omnipresent and have become a need for most of the individual activities and business life. Cyber criminals are taking advantage of this situation to carry out attack on the individuals and organization. For variety of reasons individuals become prey for cyber crime – such as lack of awareness, greediness, and carelessness, violation of security measures and non adoption of security measure. Among all these factor awareness plays a crucial role as it is the base for individual to protect them from being a victim of cybercrime. The study related to awareness on cyber crime among the user’s particularly young internet users has revealed that there is a significant difference in awareness level among users which can lead them to the victims of cyber crime [3]. Similarly, studies showed that activities leading to the awareness creation can reduce the number of cyber crime victims [4]. Most of the victims of common cyber crimes such as phishing, spamming and virus attacks are due to lack of awareness and knowledge among the users.

4. Cyber Crime in India

Cybercrime refers to criminal activities carried out through the use of a computer or internet [5]. One approach of classification of cyber crime is based on the role of computers or electronic devices in the cybercrimes and on the other way classified on the basis of victims such as individuals, crimes against property, crime against organization or crime against society [6]. The most popular cyber crimes are financial frauds, cyber terrorism, Cyber extortion, cyber warfare, attack on computers like viruses, Denial of Service Attacks, malware, attack through computer such as identity theft, information warfare, phishing scams and spam's, obscene publication and online harassments. Even though these many cyber crimes, the crimes such as phishing, spam's, viruses, bots infection on systems, data theft, pornography and cyber stalking are common in India and have a serious impact on individual information and life.

5. Data Analysis

The present study analyses the cyber crime data where computer is used as a tool for committing the crime and computer as the target of the crime. An attempt also made to analyse the data on the basis of cases registered under IPC and IT Act.

5.1 Computer as Tool for Crime

The most reported cybercrimes in India under the category computer as a tool for cybercrimes are phishing, network scanning and spam apart from other crimes that are insignificant in number so excluded from the analysis. Phishing is technique by which fraudster obtain information such as username and password for malicious purpose by projecting as a trusted entities in an electronic communication [7]. Virus is harmful software which modifies other programs by inserting its own code [8]. Data theft is process by which the stored information in the database is stolen. Network scanning is process of illegally accessing system related information by infiltrating in to the computer networks that form the base of further attacks. Spam's are unsolicited message which can contain harmful worms and viruses which when opened can get downloaded in to the system through which perpetrator can gain access to the systems.

The total security incident where computer is used as tool for crimes has increased by 54 times during the study period with a fluctuating trend over the previous year. Cyber attacks through Spam constitutes the major of total security incidents reported during the study period with 91 percent, followed by network scanning and phishing with 7 and 2 percent respectively. Out of total phishing attacks, the highest number of such attack was reported during the year 2014 which is almost twice the base year. The same trend is noted in the case of Spam with highest number being reported in the year 2014 which is almost 281 times the base year. While in the case of network scanning, the year 2017 registered highest which is almost 35 times of the base year. When comparing base and end year, it is only the phishing that has decreased while all the others security attack has increased. One of reason for such decrease may be the efforts taken by individual organizations and agencies to spread awareness on phishing over the years via advisories and training. The following table explains the cyber crimes trends relating to computer as a tool for cyber crime

Table 1: Computer as Tool for Cybercrime

Year	Phishing		Network Scanning		Spam's		Total	
	A	T (yoy)	A	T (yoy)	A	T (yoy)	A	T (yoy)
2008	604 *(51.45)	1.00	265 (22.57)	1.00	305 (25.98)	1.00	1174 (100)	1.00
2009	374 (38.88)	0.62	303 (31.50)	1.14	285 (29.63)	0.93	962 (100)	0.82
2010	508 (25.84)	0.84	477 (24.26)	1.80	981 (49.90)	3.22	1966 (100)	1.67
2011	674 (13.75)	1.12	1748 (35.66)	6.60	2480 (50.59)	8.13	4902 (100)	4.18
2012	887 (7.45)	1.47	2866 (24.08)	10.82	8150 (68.47)	26.72	11903 (100)	10.14
2013	955 (1.62)	1.58	3239 (5.50)	12.22	54677 (92.88)	179.27	58871 (100)	50.15
2014	1122 (1.25)	1.86	3317 (3.68)	12.52	85659 (95.07)	280.85	90098 (100)	76.74
2015	534 (0.81)	0.88	3673 (5.58)	13.86	61628 (93.61)	202.06	65835 (100)	56.08
2016	757 (1.30)	1.25	416 (0.71)	1.57	57262 (97.99)	187.74	58435 (100)	49.77
2017	552 (0.87)	0.91	9383 (14.75)	35.41	53692 (84.39)	176.04	63627 (100)	54.20

Source: Compiled from the Annual Reports of CERT-In
T – Trend in times year on year basis
** - Figures in the parenthesis specifies percentage to total attack.*

Further analysis reveals that the network scanning and probing activities have increased by 35.41 time compared to the base year, the probable reason may be increase in the number of internet user, that allowed the hacker to take advantage of the systems without proper security measures like original anti-virus softwares. It is important to note that as per the report by International Telecommunication Union, the number of internet user in India has increased from 92 million in the year 2010 to 390 million in 2016 and expected to reached 481 million at the end of June 2018 as per the report of Internet and Mobile Association of India[9]. In case of spam, it has almost increased 176 times when compared to base year. The increase in number of active email user (as per the report of STASTIA it is expected to reach 200 million at the end of year 2018 in India) with the corresponding increase in email usage among individuals and business community (as per report of THE RADICATI GROUP [10], INC increase in business and consumer mails sent and received per day to exceed 281 billion in year 2018) would have created an opportunity for perpetrators to carry out attacks through spam's.

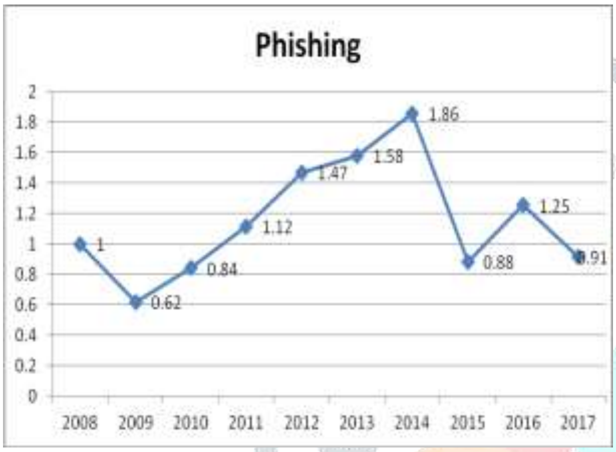


Fig.1

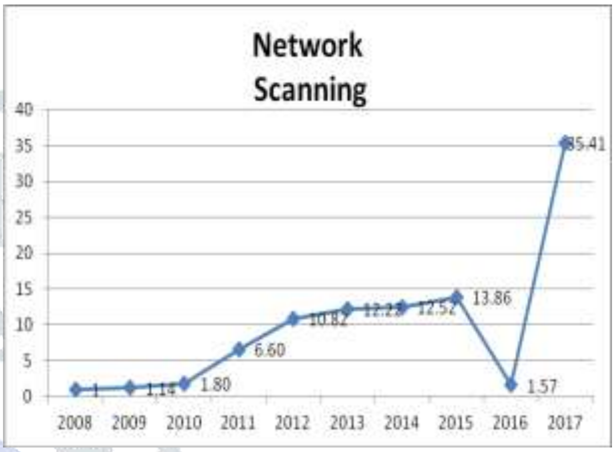


Fig .2

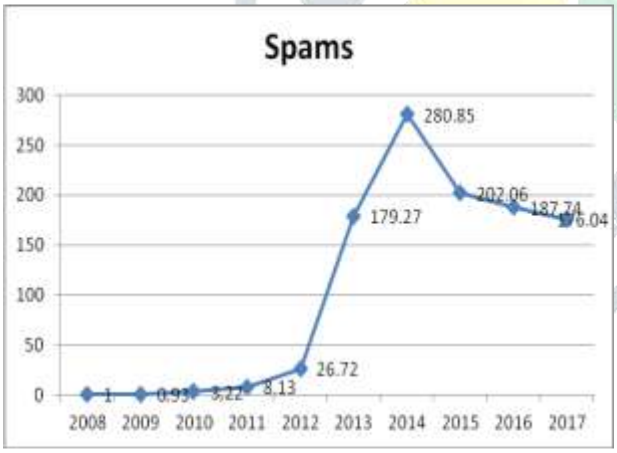


Fig. 3

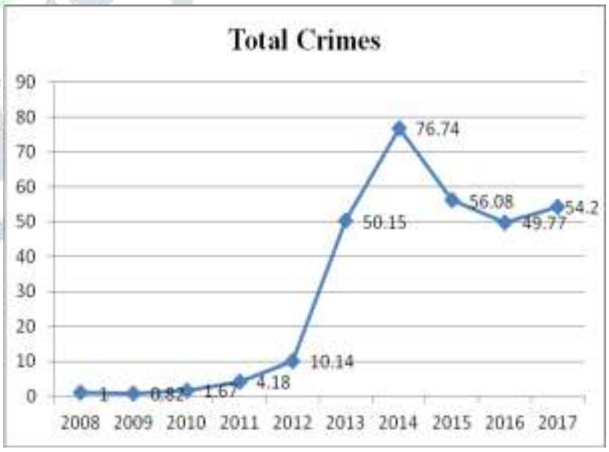


Fig. 4

As per fig.1 and fig.2 Phishing attack shows a fluctuating but increasing trend while in case of network scanning it is of increasing nature except for the year 2016. As per fig.3, after an initial decrease, trend related to spam's shows a linear increase up to certain year followed by the linear decrease. In case of total number of crimes as portrayed in the fig. 4, after an initial decrease there was a linear increase up to certain year followed by the decrease for few years and started increasing again. The interesting fact to be noted from the above figures is that once an attack reached its high, there is a steep fall in such attacks on the following year. The probable reason may be efforts taken by agency like Cert- In in collaboration with others stake holders to prevent such attacks based on their previous experience.

5.2 Computer as a Target of crime

The most reported cybercrimes in India under the category computer as a target of cybercrimes are virus, bots infection, website defacement, malware and open proxy server. Virus is types of malicious software when executed either corrupt the system or destroy the data associated with systems. Website defacement is an attack on the websites that changes the visual appearance of the websites, usually attackers replace the original website with one of their own [11] .Bots is the software application that runs automated scripts over the internet which can be used to carry out attacks [12] .

Table 2: Computer as a Target for Cyber Crime

Year	Website Defacement		Bots Infected Systems		Website compromise & Malware Propagation		Virus & Malicious code		**others	
	A	T	A	T	A	T	A	T	A	T
2008	5.48	-	146.89	-	0.84	-	0.41	-	0.15	-
2009	6.02	1.10	3509.17	23.89	6.55	7.84	0.60	1.46	0.16	1.08
2010	14.35	2.62	6893.81	46.93	6.34	7.60	1.82	4.45	0.19	1.27
2011	17.31	3.16	6277.94	42.74	4.39	5.26	2.77	6.78	1.24	8.38
2012	23.01	4.20	6494.72	44.21	4.59	5.50	3.15	7.72	2.42	16.33
2013	24.22	4.42	7457.02	50.77	5.27	6.31	4.16	10.20	3.48	23.54
2014	25.04	4.57	7728.41	52.61	7.29	8.73	4.31	10.56	3.61	24.39
2015	26.24	4.79	9163.29	62.38	0.96	1.15	9.83	24.09	8.21	55.49
2016	31.66	5.78	10020.95	68.22	1.48	1.78	13.37	32.77	2.67	18.05
2017	29.52	5.39	18077.19	123.07	0.56	0.67	9.75	23.90	3.32	22.40

Source : Annual Reports of Indian-Computer Emergency Response Team

** Other includes attack such as DOS, DDos attack

T – Trend in times year on year basis

The data from the table 2 reveals that bots infection on system are of serious concern as number of such attacks has increased almost 123 times from the base year. As per fig.5, bots infected system shows an increasing trend except for the year 2011. In case of website defacement the number has almost increased by 5.4 time when to compare to the base year with highest number of attack happened in the year 2016 which is 5.8 times more than base year . While the number of website have increased and reached 1.76 billion worldwide (net craft and internet live stats report [13]), the corresponding attack on websites has

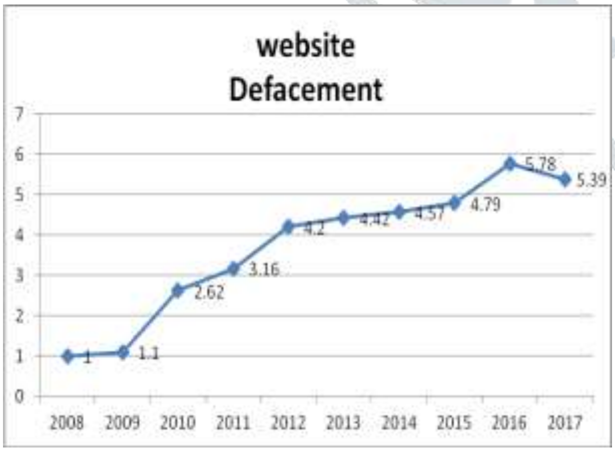


Fig.5

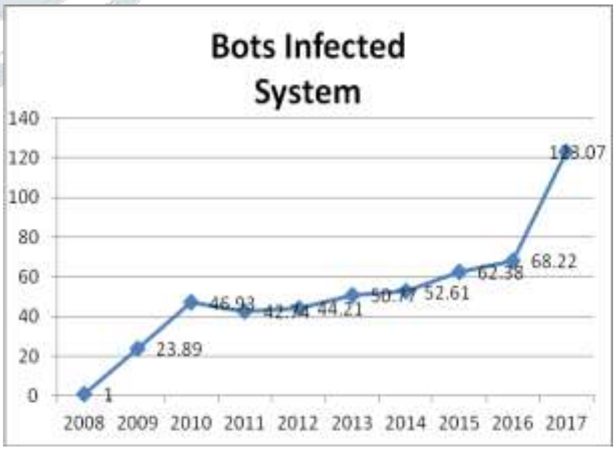


Fig.6

Increased due to the vulnerable software design (as Per Menlo security web report [14]). This can be a possible reason for constant increase on web based attack. As per fig.6 the trend related to web defacement shows a linear increasing trend up to year 2016 followed by the moderate decrease. The number of compromised websites has decreased by 0.7 time compared to base year, which may due to constant efforts taken by various agencies in identifying and preventing such attacks.

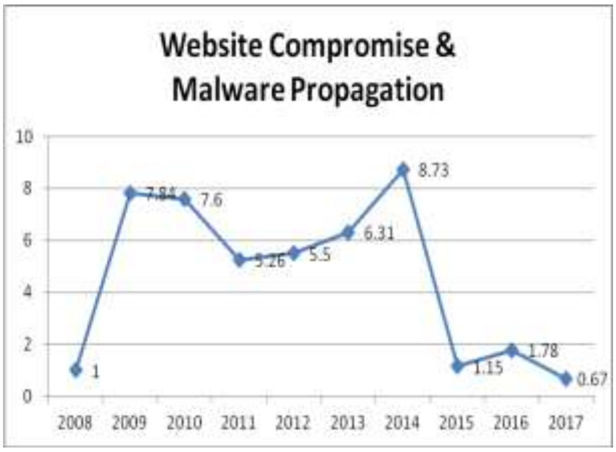


Fig.7

(Annual Reports of CERT-IN). As per fig.8 virus related attack saw a linear increase up to the year 2016 followed by the decrease in the final year of the study. When compared to base year it has increased by approximately 24 times with highest number of attacks recorded in the year 2016. It may be due to perpetrators shifting the focus to find new means to carry out attacks on computers, which is evident from increase in other attack that is almost 22.4 time the base year. The reason for the shift may probably due to efforts taken by organization and agencies in preventing existing attacks. Interesting fact to be noted here is most of attack targeting computer and computer network is on high between the period 2014 to 2016 which correspond to period when government of India initiated Make in India and digital India. As individual and small business has started digitalizing their business, attack on them would have increased which might be the probable reason for increase in attacks during such period.

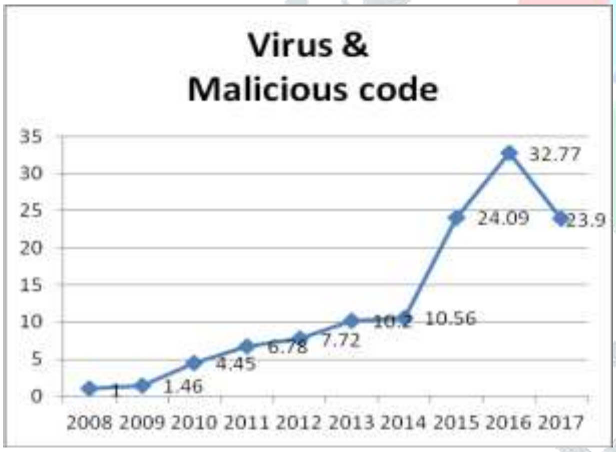


Fig.8

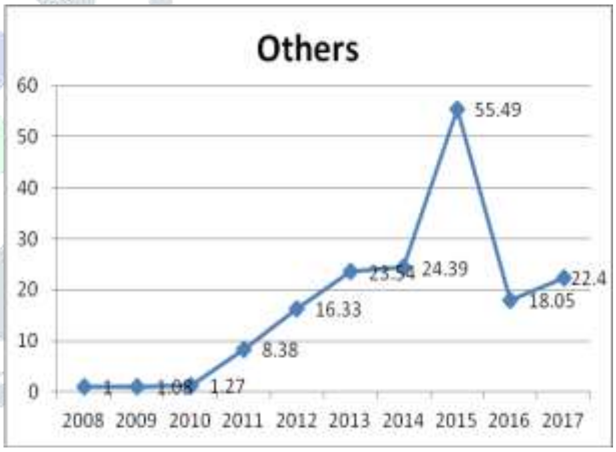


Fig 9

5.3 Domain's Specific Attack

Websites Defacement is attack carried on the organizations websites to degrade its image, thereby creating a sense of insecurity among the visitors to avoid transaction with such organization leading to business and reputational loss. Some of the most common domain name in practice are (.com) for commercial organization, (.in) India's internet country code (.org) for non profit organization and (.net) for organization like internet service provider's. The Table below list out the attacks carried on specific domains for the period 2008 to 2017.

Table 3: Defacement Of website Domain

Year	Domain Attacked										Total	
	.com		.in		.org		.net		Others*			
	A	T	A	T	A	T	A	T	A	T	A	T
2008	1916 (35.00)	-	3042 (55.56)	-	305 (5.57)	-	172 (3.14)	-	40 (0.73)	-	5475 (100)	

2009	2446 (40.61)	1.28	3089 (51.29)	1.02	238 (3.95)	0.78	166 (2.76)	0.97	84 (1.39)	2.10	6023 (100)	1.10
2010	3854 (26.86)	2.01	9772 (68.11)	3.21	447 (3.12)	1.47	221 (1.54)	1.28	54 (0.38)	1.35	14348 (100)	2.62
2011	6335 (36.61)	3.31	9839 (56.85)	3.23	663 (3.83)	2.17	311 (1.80)	1.81	158 (0.91)	3.95	17306 (100)	3.16
2012	10356 (45.00)	5.41	11277 (49.00)	3.71	690 (3.00)	2.26	460 (2.00)	2.67	231 (1.00)	5.78	23014 (100)	4.20
2013	7023 (29.00)	3.67	15490 (63.97)	5.09	969 (4.00)	3.18	246 (1.02)	1.43	488 (2.02)	12.20	24216 (100)	4.42
2014	6510 (26.00)	3.40	16274 (65.00)	5.35	1252 (5.00)	4.10	250 (1.02)	1.45	751 (3.00)	18.78	25037 (100)	4.57
2015	4665 (17.78)	2.43	18403 (70.12)	6.05	2326 (8.86)	7.63	203 (0.77)	1.18	647 (2.47)	16.18	26244 (100)	4.79
2016	10811 (34.14)	5.64	17178 (54.25)	5.65	2282 (7.21)	7.48	907 (2.86	5.27	486 (1.53)	12.15	31664 (100)	5.78
2017	9081 (30.78)	4.74	17588 (59.61)	5.78	2062 (6.99)	6.76	419 (1.42)	2.44	354 (1.20)	8.85	29504 (100)	5.39

Source : Annual Reports of Indian-computer Emergency Response Team
*Others includes attacks on .info,.biz,.edu,.name, A- Number's in Actual
T – Trend in times year on year basis
** - Figures in the parenthesis specifies percentage to total attack.*

The analysis reveals that total attack on web domains has increased by 5.4 times from base year with a linear increase up to 2016 followed by a moderate decrease in the year 2017. Of total number of attacks carried on different domains, 91 percent of attack has been on .in and .com domains. The reason being most of the Commercial organization has registered under the domain name .com, while attacking such organization can provide financial gains to perpetrators in order for restoring websites to original status or from the organization's competitors for damaging the reputations. The attack on .in domains is almost about 60 percent of total attack. One of the possible reasons may be the increase in number of .in domains to 2.01 million since 2004 (as per the record of .IN registry of National Internet Exchange of India [15]) as part of the Indian government to promote .in usage .As per fig 10

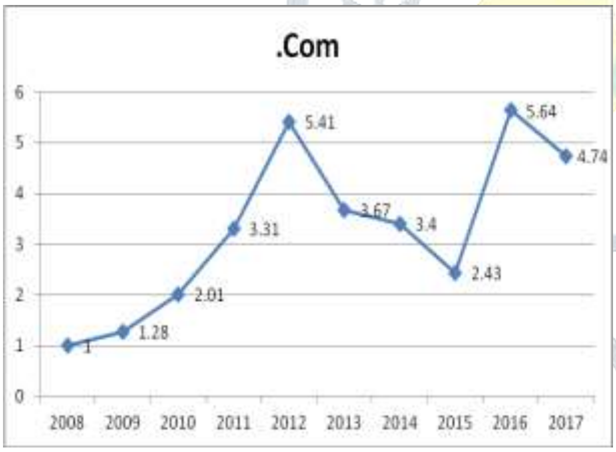


Fig 10

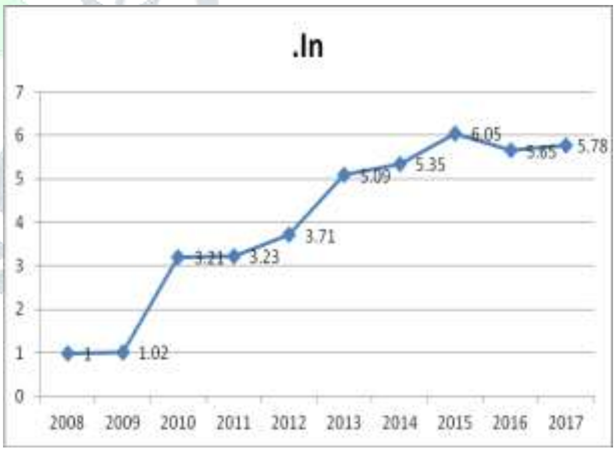


Fig 11

the total tack on .com has increased by 4.74 times with highest number of attack reported in the year 2012. In case of .in domain it has increased by 5.8 time with highest being recorded in the year 2015. The attacks on .org domain has increased by 6.76 time with highest number reported in the year 2015 where as in case of .net total number of attacks has increased by 2.4 time with highest recorded in the year 2016. From the observation it is clear that highest number of attacks on individual domain has happened between the year 2014 and 2016. The possible reason may be government initiative in terms of make in India [sep,2014] and digital India [jul,2015] that would had an impact on the individual and organization to go digital leading to increase in number of website with corresponding increase in attacks. In case of total attack related to domains the trend shows an linear

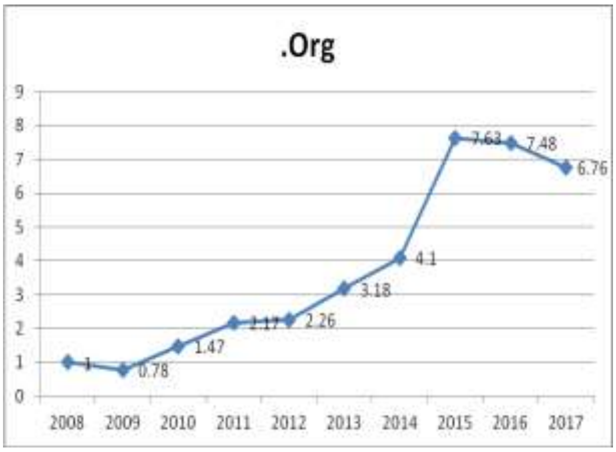


Fig 12

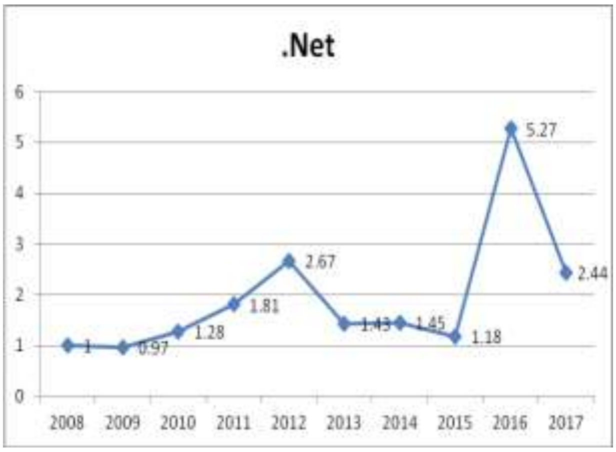


Fig 13

increase with a moderate decrease in year 2017. As per Fig 14 attack on various domains such as .info, .biz, .edu, .name represented as others show an linear increasing trend after a initial fall followed by a linear decreasing trend.

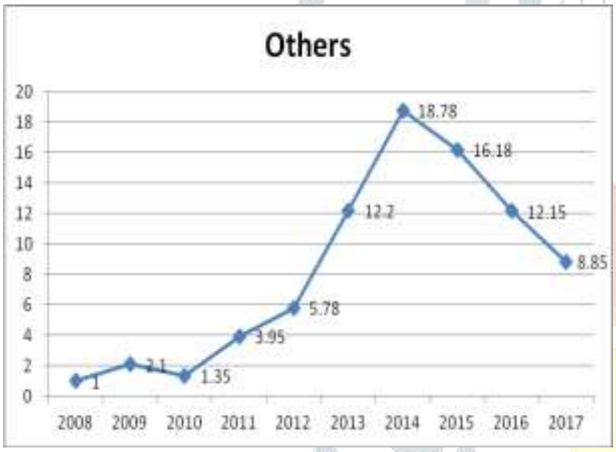


Fig 14

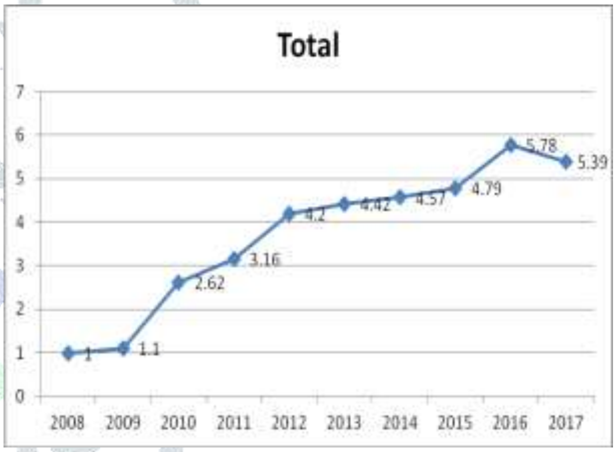


Fig 15

6. Cyber Crimes Registered under IT ACT 2000

To provide legal recognition to electronic transaction and online filling of documents with government agencies, Information Technology Act, 2000 was passed on 9th June 2000. This act contains 13 chapters and 4 schedules covering 94 section recognizing electronic transaction, digital signature to cyber offenses and punishment. This act was amended in the year 2008 and notified in the gazette as Information Technology (Amendment) Act, 2008 with certain changes in definitions, punishments and administrative power. Besides it empowers central government to create nodal agencies to protect India's information infrastructure.

The following table provides the details of the crimes registered under IT Act for the period between 2007 and 2016. For the purpose of the analysis the crimes registered under this act has been classified into computer related offences, obscene related offences, information compliance and breach related offenses and other offences that includes all the other crimes that does not fall under the first three categories.

Table 4: Cybercrime Incidence Under IT ACT 2000

Year	*Computer Related Offences		Obscene Publishing/Trans mission		**Information Breach and Non compliance		***Others		Total	
	A	T	A	T	A	T	A	T	A	T

2007	91 #(41.94)	-	99 (45.62)	-	11 (5.07)	-	16 (7.37)	-	217 (100)	-
2008	167 (57.99)	1.84	105 (36.46)	1.06	8 (2.78)	0.73	8 (2.78)	0.50	288 (100)	1.33
2009	261 (62.14)	2.87	139 (33.10)	1.40	10 (2.38)	0.91	10 (2.38)	0.63	420 (100)	1.94
2010	577 (59.73)	6.34	328 (33.95)	3.31	15 (1.55)	1.36	46 (4.76)	2.88	966 (100)	4.45
2011	1082 (60.41)	11.89	496 (27.69)	5.01	29 (1.62)	2.64	184 (10.27)	11.50	1791 (100)	8.25
2012	2039 (70.90)	22.41	589 (20.48)	5.95	49 (1.70)	4.45	199 (6.92)	12.44	2876 (100)	13.25
2013	2680 (61.52)	29.45	1203 (27.62)	12.15	99 (2.27)	9.00	374 (8.59)	23.38	4356 (100)	20.07
2014	5637 (78.28)	61.95	758 (10.53)	7.66	21 (0.29)	1.91	785 (10.90)	49.06	7201 (100)	33.18
2015	6655 (82.84)	73.13	816 (10.16)	8.24	24 (0.30)	2.18	539 (6.71)	33.69	8034 (100)	37.02
2016	6896 (80.07)	75.78	957 (11.11)	9.67	35 (0.41)	3.18	725 (8.42)	45.31	8613 (100)	39.69

Source : Reports of National Crime Record Bureau

A- Number's in Actual

T – Trend in times year on year basis

# - Figures in the parenthesis specifies percentage to total attack.

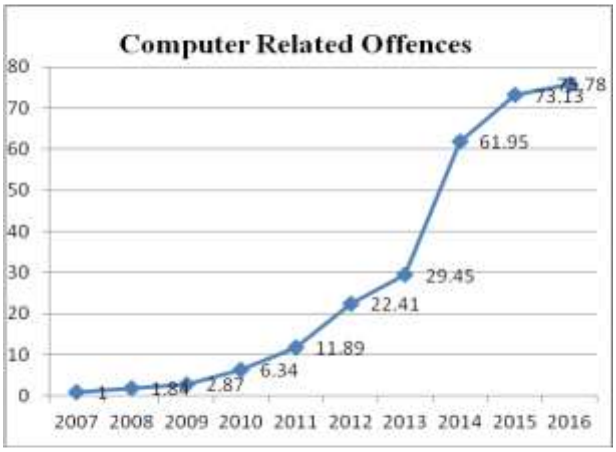
** includes tampering of computer source, hacking, loss or damage to computer resources, sending offensive message, identity theft, impersonating, violation of privacy, dishonestly receiving stolen computers, unauthorized to access computer*

*** includes breach of confidentiality, failure to block information, disclosure of information and failure to provide/ monitor/ intercept/ decrypt information.*

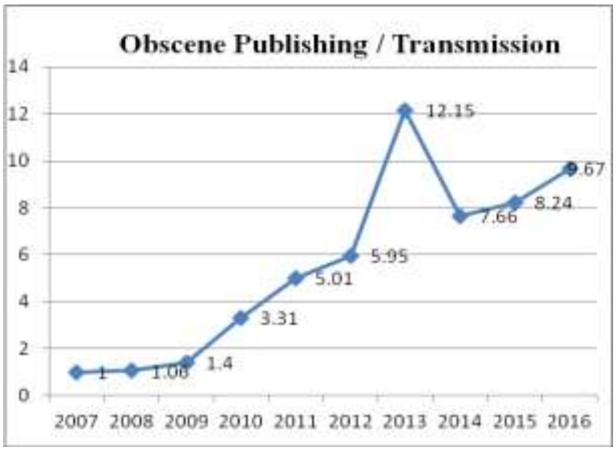
**** Other includes cyber terrorism, non compliance order of certifying authority, introducing virus worm, online share trading fraud , Obtaining Digital signature through misrepresentation ,Publishing False digital signature certificate and fraud digital certificate etc.*

The analysis of data shows a linear increasing trend with regard to total number of crime register under the IT act with an increase of 39.69 times since 2007. As per Fig16 the same trend is reflected on computer related offences with an increase being 75.78 times compared to the base year. Computer related crime tops the list with 75 percent of total crimes registered followed by the crimes related to obscene publication and transmission with 15.8 percent of total cases registered. These two crimes constituted almost 91 percent of total crimes registered under IT act 2000. The reasons behind increase in such attacks may be due to increase in number of computer and internet user without basic knowledge on safe usage [based on analysis on NSSO data published in The Hindu [16]] as well as adoption of associated security measure. Increase in cases related to obscene publication or transmission, may be due to revenge and extortion attitude of individual which is evident from the increase in number of cases registered under these categories [Analysis based on NCRB data]. As per fig 17 the number of cases registered under obscene publishing and transmission shows an increasing trend except for the decrease in the year 2014, with a highest being recorded in the year 2013.

There is also a steep increase in the cases registered under the obscene publishing and transmission for the year 2013, one of the probable reason may be increase in revenge attitude of the perpetrators as well as poor attitude of victims to contact law enforcement agencies. The steep fall in the year 2014 may be due to stringent action taken by the law enforcement agencies in terms of conviction. As per fig 18 cases related to information breach and non compliance has shown an increasing trend except for the year 2008 and 2014 with a highest fall being 4.71 times the previous year in 2014. It is the same trend observed in case of crimes under other categories except for the change in year being 2015 with a moderate decrease of 1.45 times compared to its previous year.



ig 16



F

Fig 17

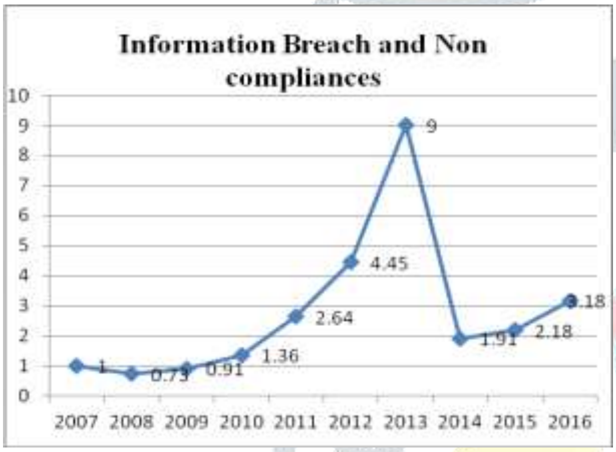


Fig 16

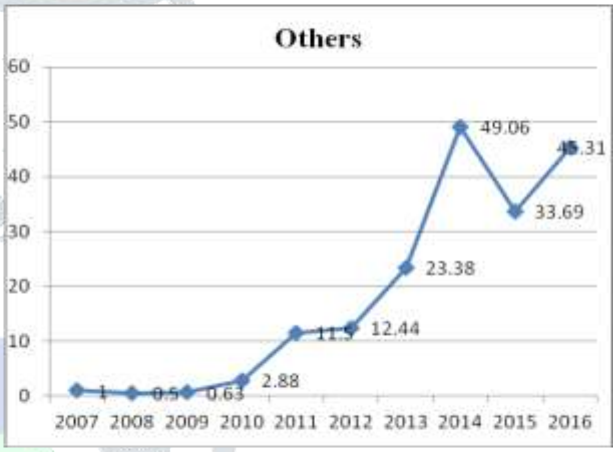


Fig 17

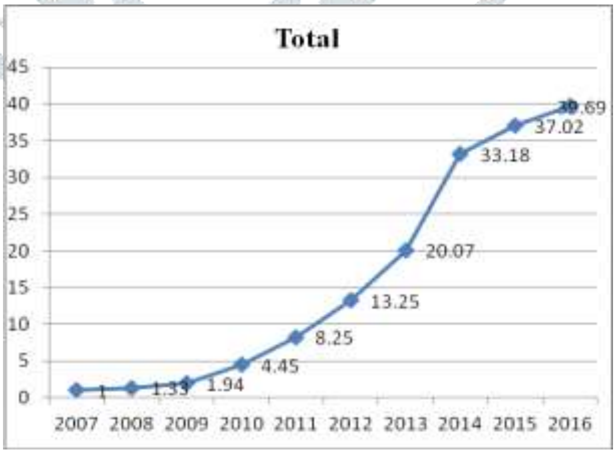


Fig 20

7. Cyber Crime Registered under IPC

The Indian Penal Code is the primary and comprehensive criminal code covering different aspect of criminal law of India. The following table provides the data related to number of cyber crime registered under IPC and SLL. SLL are special and local laws which are acts framed by the state government for special issues.

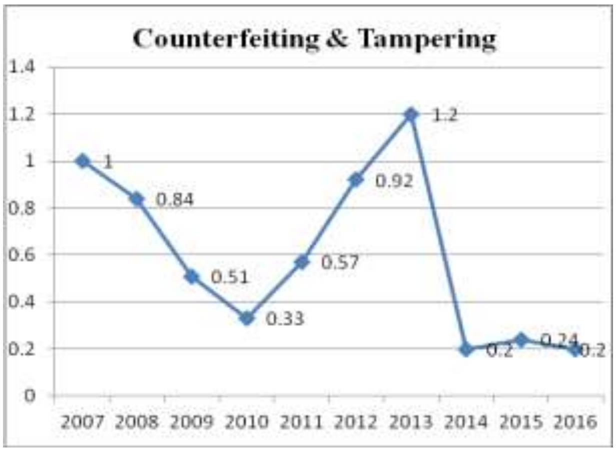
Table 5: Cybercrime Incidence under IPC

Year	*Counterfeiting and Tampering		Data Theft		**Others		Total	
	A	T	A	T	A	T	A	T
2007	49 #(14.45)	-	217 (64.01)	-	73 (21.53)	-	339 (100)	-
2008	41 (23.30)	0.84	55 (31.25)	0.25	80 (45.45)	1.10	176 (100)	0.52
2009	25 (9.06)	0.51	158 (57.25)	0.73	93 (33.70)	1.27	276 (100)	0.81
2010	16 (4.52)	0.33	188 (53.11)	0.87	150 (42.37)	2.05	356 (100)	1.05
2011	28 (6.64)	0.57	259 (61.37)	1.19	135 (31.99)	1.85	422 (100)	1.24
2012	45 (7.49)	0.92	259 (43.09)	1.19	297 (49.42)	4.07	601 (100)	1.77
2013	59 (4.41)	1.20	747 (55.87)	3.44	531 (39.72)	7.27	1337 (100)	3.94
2014	10 (0.39)	0.20	1233 (48.56)	5.68	1296 (51.04)	17.75	2539 (100)	7.49
2015	12 (0.33)	0.24	2384 (65.14)	10.99	1264 (34.54)	17.32	3660 (100)	10.80
2016	10 (.26)	0.20	2496 (64.25)	11.50	1379 (35.50)	18.89	3885 (100)	11.46

Source : Reports of National Crime Record Bureau
A- Number's in Actual
T – Trend in times year on year basis
# - Figures in the parenthesis specifies percentage to total attack.
* Crimes related to counterfeiting and tampering of property marks and Counterfeiting of currency or stamps
** includes Offense by public servant or against him and SLL crime like copy right and destruction of electronic evidence and providing false electronic evidence

Total number of crimes registered under IPC and SLL has increased by 11.46 times during the study period. The trend shows a linear increase after an initial fall in the year 2008. Similar pattern is observed in Crimes related to data theft with highest number of cases registered in the year 2016.The possible reasons behind such increase may be due to lack of awareness and attitude among the users and increase in number of attacks such as phishing and spam's [CERT-In Annual Reports] that aim to collect personal confidential information for financial gain.

While cases related to counterfeiting and tampering has decreased by 0.20 times, the cases registered under other categories have increased by 18.89 times and shows an increasing trend except for the moderate decrease in the year 2011 and 2015.The main reason behind such an increase may be the increase of SLL crimes in recent years. Of total number of crime registered 59 percent of crime is related to data theft which is due to the financial gain from such data.



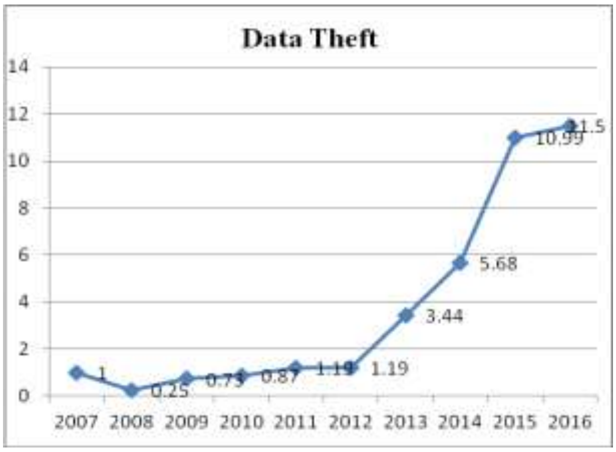


Fig 21

Fig 22

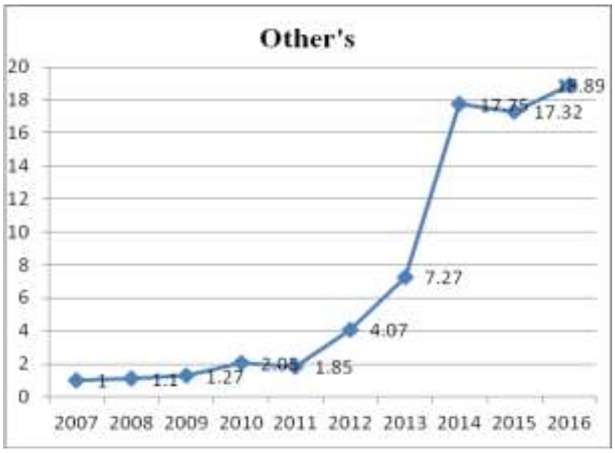


Fig 23

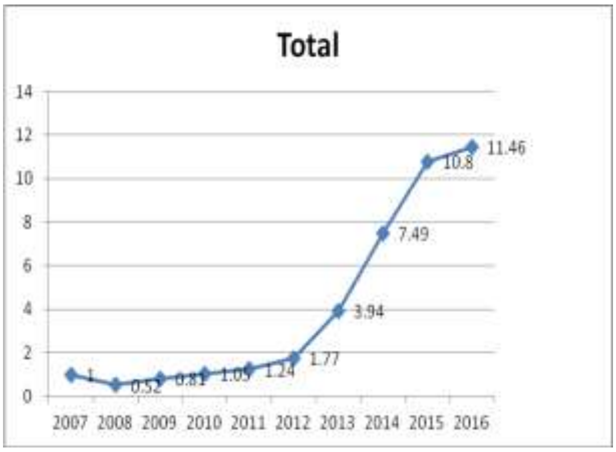


Fig 24

Summary of Findings

- Spam's constitutes the major of total security incidents reported using computer as a tool with 91 percent, followed by network scanning and phishing with 7 and 2 percent respectively.
- The bots infected system has increased by 123 percent followed by denial of service attack with 22.40 per cent, viruses and website defacement with 23.90 per cent and 5.39 percent respectively.
- The attacks on web domains have increased by 5.4 times. Of total number of attacks carried on different domains, 91 percent of attack has been on .in and .com domains.
- Total cases registered under IT act have increased by 36.69 percent with computer related offenses tops the list with 75.78 percent followed by other category crimes, obscene publication and information breach.
- Total number of cases registered under IPC Act has increased by 11.40 percent.

Conclusion

With the explosion of information and communication technology and indiscriminate use of technology by individuals and institutions facilitates the cyber criminals to thrive in the cyber space and spread their misdeeds in the recent times. It is a great challenge for the netizens and institutions to protect and secure their property, information and data from such cyber rogues. The numbers presented in data may not describe the real problem as the reporting of crimes is very poor in India and across countries because of lack of awareness and knowledge about victimisation. Though the governments across the different geographies were making the various efforts through legislation, institutions, law enforcement, tools and techniques to control the cybercrimes it remained as a great challenge for the global community. It is the individual and organisational efforts to create awareness, better behaviour in the cyberspace by the users and positive use of technology only can help the cyberspace a better place for the user community.

Reference

[1] https://www.itu.int/en/mediacentre/Pages/2016-PR30.aspx accessed on October 08, 2018

[2]https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/ accessed on October 08, 2018

[3]M. S. Hasan, R. A. Rahman, S. F. H. B. T. Abdillah, and N. Omar, "Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia," *J. Soc. Sci.*, vol. 11, no. 4, pp. 395–404, 2015

[4]Choi, K., 2008. Structural equation modeling assesment of key causal factors in computer crime victimization. Ph.D Dissertation, Indiana University of Pennsylvania, USA

[5]http://www.oxforddictionaries.com/definition/english/cybercrime (Accessed on 28th august, 2018)

[6] Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley. p. 392. ISBN 0-201-70719-5

[7] Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark & Stavroulakis, Peter. *Handbook of Information and Communication Security*. Springer. ISBN 978-3-642-04117-4.

[8] Stallings, William (2012). *Computer security : principles and practice*. Boston: Pearson. p. 182. ISBN 978-0-13-277506-9

[9]Https://cms.iamai.in/Content/ResearchPapers/2b08cce4-e571-4cfe-9f8b-86435a12ed17.pdf

[10] http://www.radicati.com/wp/wp-content/uploads/2017/01/Email-Statistics-Report-2017-2021-Executive-Summary.pdf

[11] https://en.wikipedia.org/wiki/Website_defacement (Accessed on 28th Sep, 2018)

[12] https://techterms.com/definition/bot (Accessed on 28th Sep., 2018)

[13] http://www.internetlivestats.com/total-number-of-websites (Accessed on 5th Oct, 2018)

[14] https://www.infosecurity-magazine.com/news/42-of-the-webs-top-sites-are (Accessed on 5th Oct, 2018)

[15] https://registry.in(Accessed on 15th Oct, 2018)

[16]https://www.thehindu.com/data/on-computing-ability-rural-india-is-lost-in-the-woods/article17463258.ece , (Accessed on 25th Oct, 2018)

[17]CERT-In Annual Reports [2008-2017]

[18]NCRB Annual Reports [2007-2016]