P: ISSN No. 0976-8602 RNI No.UPENG/2012/4262 VOL.-8, ISSUE-2 (Part-1) April 2019

E: ISSN No. 2349-9443 Asian Resonance

Emerging Issues of Cyber Crime in The Era of Cyberspace: Challenges and Way Forward

Monica Narang
Sr. Assistant Professor,
The Law School,
University of Jammu,
Jammu, India

Sonam Prashar
Research Scholar,
Dept. of Law,
University of Jammu,
Jammu, India

Abstract

Cyber crimes are increasing with every passing day. Necessary measures are being taken by the government and other agencies to prevent cyber related crimes but the problem keeps looming besides all the measures being taken. As it is well known that earlier cyber crimes were limited to a computer and an internet connection, but with the advancement of technology cyber crimes have entered our smart phones and most of the smart electronic devices that could be controlled with an internet connection. Hacking, e- mail bombings, data diddling or forging documents can all be done in the cyber world. 'Salami Attack' is a new trend in cyber world where small amount of theft is done by way of wrong data entry and people don't even realize that they have been cheated upon. Other emerging issues in committing cyber crimes including internet time theft, logic bombs, virus attacks, worm attack, Trojan attack, lottery frauds, cyber pornography, and child pornography are discussed in detail in the paper by the researchers. The paper also discusses extension of cyber crime to the intellectual property, stealing of copyrights and trade secrets being the most common. The unregulated or poorly regulated cyberspace has provided suitable platform to cyber terrorist and cyber mafia. Invisibility of offender while committing the crime, easy or no preparation, and privacy are some of the common reasons responsible for making cyberspace vulnerable. The fact that the offender can commit the crime single handedly makes cyber crimes even much easier to commit. The offenders could be anyone including children, professionals, discontented employees or any person known with whom the crime has been committed, and is as such discussed in the paper. Since cybercrime often has an international dimension, the researchers' stresses on thorough analysis of current legal framework to identify any possible gaps so that the perpetrators should not go unpunished due to want of legal provisions in both domestic and foreign jurisdictions. The researchers, however, suggests that the issue of cyber security can only be addressed through a multi-pronged strategy taking into account the role of different stakeholders.

Keywords: Cyberspace, Cyber Bullying, Cyber Stalking, Hacking, Cyber Frauds, Virus Attacks, Cyber Pornography, Intellectual Property Theft, Legal Framework.

Introduction

Crime is a universal phenomenon. It is prevalent in both primitive and modern societies alike though with different forms and ramifications. No doubt since the beginning of 21st century humankind has made remarkable achievement in every sphere of life, be it social, political, cultural, technological or scientific, but the associated problem that is causing serious concern is the rapid increase in the nature and types of crimes as well. One such instance is the emergence of cybercrimes that deeply impinges upon every sphere of an individual's life. As the new world of internet expands its spheres, it also has left the society vulnerable to an altogether new set of crimes. Cyber crimes are increasing with every passing day. As it is known that earlier cyber crimes were limited to a computer and an internet connection, but with the advancement of technology cyber crimes have entered our smart phones and most of the smart electronic devices that could be controlled with an internet connection. Hacking, e mail bombings, data diddling or forging documents can all be done in the cyber world. 'Salami Attack' is a new trend in cyber world where small amount of theft is done by way of wrong data entry and

people don't even realize that they have been cheated upon. Other various emerging trends in committing cyber crimes includes internet time theft, logic bombs, virus attacks, worm attack, Trojan attack, lottery frauds, email spoofing , phishing and child pornography. The extension of cyber crimes to intellectual properties is also widespread, stealing of copyrights and trade secrets being the most common**.** The poorly regulated cyberspace has provided suitable platform to cyber terrorists and cyber mafia.

The incidence of cyber crimes under the IT Act, 2000 has increased by 457% from the year 2011 to 2016 in India, whereas the increase in incidence of the crime under IPC has also increased as compared to the year 2017.[1] Bengaluru has the second highest number of cybercrime cases among the metros, behind Mumbai with 980 cases. Maharashtra has emerged as the center of cyber crime with maximum number of incidence of registered cases under cyber crimes. Hyderabad records 291 cases, Kolkata 168, Delhi 90 and Chennai 36 cases. From 762 to 5,035, the number of cases has seen a sharp increase in Bengaluru. Bengaluru registered the most number of cyber crimes in 2018. 5,035 FIR's were registered at a lone cybercrime police station in the city. 2,945 cases were registered in the state of Maharashtra till September 2018, most of them in Mumbai.[2] Symantec Corp ranked India among top five countries to be affected by cyber crimes from 2012 to 2017.[3] The rapid surge in cyber crimes can be attributable to the reason that they possess the lack of respect for jurisdictional boundaries, openness to participation, the potential for anonymity of members of the virtual community, and its apparent economic efficiency.[4]

Aim of the Study

The aim of this study is to coordinate various efforts relating to cyber crime, prevention and regulation. Basic Aim to provide assistance to law enforcement agencies and contribute to the fight against cyber crime in India for detection, investigation and prosecution.

Review of Literature

In this paper, the authors have consulted books on cyber Crime by Peter Grabosky and G. Broadhurst, Hong Kong University Press (2005), P.K. Singh, Book Enclave (2007), Book by Sushma Arora and Raman Arora, Taxmann (2019). The researcher has also taken information from reputed journals, internet and also related The Information Technology Act 2000 and Indian Penal Code.

What Are Cyber Crimes

With the advancement of technology the man is getting more and more dependent on Internet for all the needs as Internet gives easy access to everything while sitting at the comfort of our home. Through the medium of internet, social networking has emerged as a trend, online shopping is increasing at an enormous rate, and gaming has become favorite part time leisure. Online studying and even online jobs, every possible thing that we can think of can be done by the way of an internet connection. The number of internet users in India is 420 million as of June 2017[5], of which India is placed third after US and China. The number of internet users may reach 500 million by June 2018, according to a report.[6] With the development of the internet and its related benefits the concept of cyber crimes is developing at the same pace.

Cyber crimes can be defined as the unlawful acts where the computer is the object of crime. Computer is used either as a tool or a target or both. The term is a general term that covers crimes like phishing, credit card frauds, bank robbery and so on.[7]

Cyber crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity.[8]

Cyber crime is a generic term that refers to all criminal activities done using the medium of computers, the Internet, cyber space and the worldwide web.[9] Thus, the computer may have been used in the commission of a crime, or it may be the target. Overall result is the criminal exploitation of the Internet.

The Thirteenth United Nations Congress on the Prevention of Crime and Treatment of Offenders[10] addressed the issues of crimes related to computer networks, divided cybercrime into two categories and defined it as:

1. Cybercrime in a narrow sense (computer crime) is an illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.
2. Cybercrime in a broader sense (computer-related crime) is an illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

In simple words, cybercrime could be defined as a criminal activity that involves a computer or any networking device along with an internet connection. Cybercrimes mainly focuses on financial gain to the offender and sometimes they are meant to hurt the victim. In cyber world individuals and businesses both can become targets of cyber crimes.

Different Types of Cyber Crimes

Cyber Crimes can be categorized[11] in four ways:

The Crimes in Which the Computer Is the Target

Examples of such crimes are hacking, virus attacks, DOS attack etc.

The Crimes in Which the Computer Is Used As A Weapon

These types of crimes include cyber terrorism, IPR violations, credit card frauds, EFT frauds, pornography etc.

Computer is Incidental to Other Crimes

Money laundering and unlawful banking transactions, organized crime records etc.

Crimes Associated With the Prevalence of Computer

Software piracy, counterfeiting, copyright violation of computer programs, theft of technological equipment etc.

The most prevalent cybercrimes includes[12]:

Hacking

This is an act committed by an intruder. The intruder accesses somebody else's computer system without permission. Hackers are usually computer programmers. They have advanced understanding of computer and misuse that knowledge. Due to hacking there is loss of data as well as computer.

Botnets

A botnet is a collection of internet-connected devices, which includes computers, mobile devices that have been infected with a bot. A bot is a form of malware that allows a remote machine to use the resources on your computer to carry out actions. Distributed denial of service attacks (DDoS attacks) are the most recognizable use of botnets. For those computer is used as a weapon. The term botnet is derived from the words robot and network. That said, a botnet can be used for many purposes. Any action that requires a lot of computing resources is best for a botnet. In some cases, they are used to carry out ad fraud, which is when fake traffic is sent to an advertisement, and crypto mining.[13]

Logic bombs/ slag code

A logic bomb or slag code is a piece of code. It is inserted into software application or operating system to execute a malicious task after it is triggered by a specific event. It is not a virus. The infamous "Friday the 13th" virus attacked the host system only on specific dates. They perform actions like corrupting or altering data, deleting important files etc.[14]

Ransom Ware

Ransom ware, which we provided an example of in the section above, is one of the most dangerous online threats. It's a form of malware that searches your data and encrypts it, holding it hostage until you pay a ransom. In its case, your computer is the target. Most ransom ware cases ask for around $300 to be paid in crypto currency over Tor. WannaCry's demands, for example, ranged from $300-$600. Even after paying the ransom, though, your data may still be at risk.

The WannaCry Ransomware Attack

The WannaCry ransom ware attack was carried out in May 2017, infecting over 300,000 computers in 150 countries. In each case, it demanded payment of $300-$600 to unlock data it had encrypted. It is a worm that spreads by exploiting vulnerabilities in the Windows operating system. WannaCry used an exploit developed by the NSA (National Security Agency) against a Windows vulnerability in legacy versions of SMB.[15]

Browser Hijacking[16]

Browser hijacking is a cybercrime that is used for advertisement fraud. Malware hijacks the browser settings and many times change the homepage. Ad fraud falls into the category of using your computer as an accessory. Browser hijacking is common, mainly because many people don't know they are a victim. Hijackers are usually bundled with free applications and masquerade as a more secure way to use the internet. That isn't true, of course, and the attacker uses the misinformation to install malware on the computer system. Some browser hijackers redirect the websites, as well, which is a technique that can be used to download more malware on the system.

Fraud and Identity Theft[17]

Most cybercrime boils down to fraud and identity theft. Botnets are a form of fraud, for example, and phishing is often used for identity theft. Ransomware, botnets, phishing and browser hijackers are the most common tools used for those crimes, but there are others.[18] That's why it's important to be cautious with your information online. Even reputable companies, such as Yahoo, can be the target of massive data breaches, exposing billions of people to identity theft. If possible, it's not a bad idea to provide inaccurate information on your accounts and use a burner email address.

Unauthorized Access and Hacking

Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are the most targeted sites for the hackers.

Web Hijacking

Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.

Pornography[19]

Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and the internet pornography delivered over mobile phones.

Child Pornography[20]

The Internet is being highly used as a medium to sexually abuse children. The children are viable victim to the cyber crime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet. Pedophiles lure the children by distributing pornographic material and then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions. Sometimes Pedophiles contact children in the chat rooms posing as teenagers or a child of similar age and then they start becoming

friendlier with them and win their confidence. Then slowly pedophiles start sexual chat to help children shed their inhibitions about sex and then call them out for personal interaction. Then starts actual exploitation of the children by offering them some money, or falsely promising them good opportunities in life. The pedophiles then sexually exploit the children either by using them as sexual objects or by taking their pornographic pictures in order to sell those over the internet.

Cyber Stalking

In general terms, stalking can be termed as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim. Cyber Stalking means repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Both kind of Stalkers, either online or offline, they try to control the victims life.

Denial of Service Attack[21]

This is an attack in which the criminal floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCp/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker.

Virus Attacks

Viruses are the programs that have the capability to infect other programs and make copies of itself and spread into other program. Programs that multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attaches them to other software. Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Viruses usually affect the data on a computer, either by altering or deleting it. On the other hand worms merely make functional copies of them and do this repeatedly till they eat up all the available.

Trojan Attack[22]

Trojan Horse is a type of malicious software that looks legitimate but takes control of the computer which is attacked. it acts like something useful but do the things that are quiet damping. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.

Software Piracy

Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code or patent violations. Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws. Cyber squatters register domain name identical to popular service provider's name so as to attract their users and get benefit from them.

Salami attacks

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

Phishing[23]

Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. By spamming large groups of people, the phisher counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with legitimately.

Internet time theft

Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.

Sale of Illegal Articles

This category of cyber crimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

E-commerce/ Investment Frauds

It uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

Email Spoofing

Email spoofing refers to email that appears to originate from one source but actually has been

sent from another source. Email spoofing can also cause monetary damage.

Cyber Defamation

When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends, it is termed as cyber defamation.

Cyber Squatting

it means where two persons claim for the same Domain Name either by claiming that they had registered the name first on by right of using it before the other or using something to that previously. E.g. two similar names i.e. www.yahoo.comand, www.yaaahoo.com.

Forgery

Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high quality scanners and printers.

Email Bombing

A large number of Emails are sent to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

Theft of Computer System

This type of offence involves the theft of a computer, some parts of a computer or a peripheral attached to the computer.

Breach of Privacy and Confidentiality

Breach of privacy means unauthorized use, access, distribution or disclosure of personal information. Confidentiality means non disclosure of information to unauthorized or unwanted persons. Leakage of other type of information that is useful for business may cause damage to business or person, such information should be protected. Special techniques such as Social Engineering are commonly used to obtain confidential information. Most common breaches happen when person's information is stolen, lost or mistakenly shared.[24]

Data Diddling

Data diddling involves changing data prior or during input into a computer. The information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also includes automatic changing the financial information for some time before processing and then restoring original information.

Cyber Terrorism

Attacks that are targeted on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc. Cyber terrorism is an attractive option for modern terrorists for several reasons.

From the above discussion, we can also classify different types of cybercrimes into following headings:

1. Crime against persons (Cyber Stalking, Child Pornography, Email/SMS Spoofing, Cyber Defamation, etc.)
2. Crime against persons property (Intellectual Property crimes, Cyber Squatting, Cyber vandalism, Hacking, Transmitting virus, cyber trespass, Internet time thefts)
3. Crime against government (Cyber terrorism, Cyber warfare, Distribution of pirated software, Possession of unauthorized information etc)
4. Crime against society at large (Child Pornography, Cyber trafficking, Financial crimes, Forgery).

Indian Response to Cybercrime

With the advent of Internet, Information Highway and Cyberspace, cyber crimes are also increasing by leaps and bounds. To keep a check on the crimes we witnessed via cyberspace, Information Technology Act, 2000 was enacted. The Act has a prime objective of creating an enabling environment for commercial use of Information Technology. Punishable acts are specified in the IT Act, 2000. However, major amendments were carried out in 2006 and 2008 to deal with emerging cyber crimes.

The Indian Penal Code, 1860 has also been amended to take into its purview cyber crimes. In order to widen the scope of applicability of the provisions of the Indian Penal code so as to include within it offences involving electronic records, a new Section 29A[25] was inserted after Section 29.

As a result of this amendment all the offences related to documents also include offences related to electronic records which are committed through internet or cyberspace.

The various offences related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

Tampering with Computer source documents[26], Hacking with Computer systems, Data alteration[27], Publishing obscene information[28], Un-authorized access to protected system[29], Breach of Confidentiality and Privacy[30], Publishing false digital signature certificates[31], Sending threatening messages by email[32] Sending defamatory messages by email[33], Forgery of electronic records[34], Bogus websites, cyber frauds[35], Email spoofing[36], Web-Jacking[37], E-Mail Abuse[38], cyber stalking[39], criminal intimidation[40].

Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act, 1985 and online sale of Arms under Arms Act, 1959 also comes under the purview of cyber crimes to some extent.

Still Information Technology Act, 2000 is the primary law in India dealing with cybercrime. Though IT Act has played a very important role in the lives of people yet it has several drawbacks:

1. The term cyber- crime and cyber offence as such is not defined under IT Act, 2000.
2. IT Act does not cover the important issue of jurisdiction which is very important legal aspect in deciding the place of filing the case.
3. IT Act does not touch e-mail authenticity or its evidentiary value in the hands of receiver.

4. The concept of e-commerce is mainly based upon domain name. However, this act is silent about the domains names infringement, cyber-squatting, typo squatting, spamming and security of information at various levels.
5. Statutory bodies may not accept electronic documents. On one hand, the main aim and objective of the IT Act, 2000 was to facilitate e-governance, however on the other hand, section 9 provides that no one can insist any government office to interact in electronic form.

Conclusion

Of the common spaces known to human mind viz., Land, Water, Air and Outer Space, a new space that has marvelously emerged and virtually overtaken activities pertaining to all traditional spaces is Cyberspace. It is challenging established institutions and practices in a manner difficult to comprehend by common man. The information and communication revolution has demolished economic barriers and political boundaries and challenging the established organizations of even the developed nations. India have to make a quantum jump in law making relating to cyberspace if we want to develop capacities to protect national interests and avoid exploitation by criminals armed with technological sophistication who finds it much easier to carry their nefarious activities in cyber world. So, there is high need to regulate cyberspace. However, any feasible regulatory attempt should include a mechanism for reaching a broad international consensus. Such consensus should be multinational in its reach and hence avoid vulnerability to chauvinistic national interests or sentiments. Shifting sentiments in one national should not alter the overall definitional landscape of what is offensive or outrageous. The mechanism should also be multi-cultural in scope, in order to circumvent any charges of cultural imperialism, and to stimulate cross-cultural exchange of ideas.

Endnotes

1. *India saw 457% rise in cybercrime in five years: Study, available at: https://telecom.economictimes.indiatimes.com/news/india-saw-457-rise-in-cybercrime-in-five-years-study/67455224 (last visited on June 3, 2019).*
2. *Bengaluru is India's cybercrime capital, available at: https://economictimes.indiatimes.com/tech/internet/bengaluru-is-indias-cybercrime-capital/articleshow/67769776.cms?from=mdr(last visited on June 3, 2019).*
3. *India third most vulnerable country to cyber threats, available at: https://www.thehindu.com/news/national/india-third-most-vulnerable-country-to-cyber-threats/article23437238.ece (last visited on June 3, 2019).*
4. *P.K. Singh, Laws On Cyber Crimes Along With IT Act and Relevant Rules, Book Enclave (2007).*
5. *Number of internet users in India, The Growth Rate and Internet Penetration in India, available at: https://www.emarketeducation.in/power-internet-penetration-online-india/ (last visited on June 2, 2019).*
6. *Internet and Mobile Association of India (IAMAI) Report, 2017.*
7. *Technopedia definition of cyber crime, what is Cybercrime, available at: https://www.technopedia.com/definition/2387/cybercrime (last Visited on June 13, 2019).*
8. *G. Kumar, A. Kumar, and S. Sethi, "Computer Network Attacks- A Study" 11 International Journal of Computer Science and Mobile Applications 24-32 (2014).*
9. *R. Moore, Cyber Crime: Investigating High-Technology Computer Crime, Cleveland, Mississippi: Anderson Publishing (2005).*
10. *http://www.unodc.org/documents/congress/Documentation/ACONF222_L6_e_V1502120.pdf (last visited on may 2, 2019).*
11. *Hamid Jahankhani, Ameer Al-Nemrat, Amin Hosseinian-Far, Cyber crime Classification and Characteristics, available at: https://www.researchgate.net/publication/280488873 (last visited on June 3, 2019).*
12. *Sushma Arora & Raman Arora , Cyber crimes and cyber laws , Taxmann's, 3 edition, 2019. See also: Cybercrime: The Complete Guide to All Things criminal on the Web, available at: https://www.cloudwards.net/cybercrime (last visited on June 3, 2019).*
13. *What is botnet?-definition from whatIs.com, available at : https://searchsecurity.techtarget.com/definition/botnet (last visited on may 15, 2019).*
14. *What is a logic bomb?, available at: https://www.computerhope.com/jargon/l/logibomb.htm (last visited on april 3, 2019).*
15. *WannaCry ransomware, What is WannaCry ransomware?- Definition from whatsls.com, available at: https://searchsecurity.techtarget.com/definition/WannaCry-ransomware (last visited on may 3, 2019).*
16. *A. Razzaq, Farooq Ahmad, and M. Masood, "Cyber security: Threats, Reasons, Challenges, Methodologies and State of the Art Solutions for Industrial Applications," in Proceedings of the 2013 IEEE Eleventh International Symposium on Autonomous Decentralized systems(ISADS), pp. 1-6, Mexico City, Mexico, March 2013.*
17. *CIFAS, The UK's Fraud Prevention Service, 2012, available at: http://www.cifas.org.uk/ (last visited on June 3, 2019).*
18. *Financial Fraud Action UK, 2012. Fraud: The Facts 2012. available at: http://www.theukcardassociation.org.uk/wm_documents/Fraud_The_Facts_2012.pdf (last visited on June 1, 2019).*
19. *A. Cooper and L. Sportolari, "Romance in Cyberspace: Understanding Online Attraction", 22(1) Journal of Sex Education and Therapy, 7-14 (1997).*
20. *K. Durkin, "Misuse of Internet of Pedophiles: Implications for Law Enforcement and Probation Practice", 61(2) Federal Probation, 14-18 (1997).*

21. *The 12 Types of Cyber Crime / Chapter No. 2 / Fasttrack To Cyber Crime / Digit, available at: https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html (last visited on may 15, 2019).*
22. *What is Trojan? Is it a virus or is it a malware?, available at: https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html (last visited on may 3, 2019).*
23. *Anti-Phishing Working Group (APWG), 2013. Global Phising Survey: Tremds and Domain, available ar: http:/docs.apwg.org/reports'APWG_GlobalPhisingSurvey_1H2013.pdf (last visited on June 5, 2019).*
24. *Privacy breaches- Office of the Privacy commissioner of Canada, available at: https://www.priv.gc.ca/en/privacy-topics/privacy-breaches (last visited on June 1, 2019).*
25. *Indian Penal Code, 1860, Section 29A: Electronic Record: The Words "electronic record" shall have the meaning assigned to them in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000.*
26. *Sec.65, The Information Technology Act, 2000*
27. *Id., Sec.66.*
28. *Id., Sec.67.*
29. *Id., Sec.70.*
30. *Id., Sec.72.*
31. *Id., Sec.73.*
32. *Indian Penal Code, 1860, Sec. 503.*
33. *Id., Sec. 499.*
34. *Id., Sec. 463.*
35. *Id., Sec. 420.*
36. *Id., Sec. 463.*
37. *Id., Sec. 383.*
38. *Id., Sec. 500.*
39. *Id., Sec. 354-D.*
40. *Id., Sec. 503.*