Digital Crime and its Impact in Present Society

Yerra Shankar Rao
Department of Mathematics
Gandhi Institute of Excellent Technocrats
Bhubaneswar, India

Tarini Charana Panda
Department of Mathematics
Revenshaw University
Cuttack, India

Debasish Pradhan
Computer Science & Engineering
Einstein Academy of Technology & Management
Bhubaneswar, India

Ranjita Rath
Department of Mathematics
GIET University
Gunupur, India

***Abstract*- The facilities of computer technology have not come out without drawbacks. Though it makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'Cyber crime'without computers, entire businesses and government operations would almost cease to function. This proliferation of cheap, powerful, user-friendly computers has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. As businesses, government agencies, and individuals continue to rely on them more and more, so do the criminals Restriction of cyber crimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society. Therefore, in the current manuscript a systematic understanding of cyber crimes and their impacts over various area like Socio-eco-political, consumer trust, teenager etc.with the future trends of cyber crimes are explained.**

Keyword: cyber crimes, emotion, teenager access crime, consumer trust

I. INTRODUCTION

This study was carried out purposely to explain clearly the concept of Cybercrime and Cyber security and provide adequate and sufficient ways of getting out of these problems in the present days of internet usage and applications. The present age is the age of 'automation' where man is shifting his maximum burden on machines to get work done. The Computer Technology helps the present human civilization to such a greater extend that life without computers seem to be impossible! Speaking with examples, railway reservations, aircraft transportations, Banking transactions, all are now carried out with the help of computer machines and every data and information has acquired electronic shape and capable to move through the optic fibres.[11] Today, voice files, song files, photographs, currencies, news items, clips, bio-data's, letters, so on and so. forth are capable of being transferred, distributed, circulated and stored in electronic form. Thus present generation is greatly depends upon the computer technology for the easy mechanism and effective operations operated in electric format through computers.

Cyber crime is a term used to broadly describe 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 is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. The Cyber crime can halt any railway where it is, it may misguide the planes on its flight by misguiding with wrong signals, it may cause any important military data to fall in the hands of foreign countries, and it may halt e-media and every system can collapse within a fraction of seconds. This study was carried out purposely to explain clearly the concept of Cybercrime and Cyber security and provide adequate and sufficient ways of getting out of these problems in the present days of internet usage and applications.

II. MATERIALIZATION OF CYBER CRIME

The aftermath of World War-II has witnessed the drastic changes in every domain of life. The new mechanical adroit appear to convert all relationships of man with material things vanishing the boundaries between living and non-living being. Today mechanical adoption by human being is challenging the standards of conventional limitations laid down by time and space. The Cyber-technology has played major role in this transformation.

The present study has been undertaken to touch some aspects, effect and prospects of this Cyber-technology with special reference to threat pose by Cyber crime by India. Efforts have been made to analyze legal framework available for its control in India. To start with, it is, therefore, necessary to demarcate the dimensions of word 'crime'. Thus it is beyond doubt that 'crime' is a relative phenomenon, universal in nature and essentially all societies from ancient to modern have been evidently demonstrating its presence. Each society have been providing its own description of criminal behaviour and conduct made punishable by express will of the political community ruling over the society and it was always influence by religious-social-political economical values prevailing in the given society. Thus from time immemorial the behaviour that attracts '*penal liability*' influenced and characterized by overall outcome of these standards. Parenthetically, just as concept of crime [has undergone] change with the growth of Information Technology so the categories of criminals who engage in such crimes.3 So far Indian society is concerned,

particularly during ancient period, the definition of crime flagged by religious interpretation. The period was known for complete eminence of religion. All political and social activities in general and 'Crime' in particular, considered to be happened due to the presence of super-natural power. The Demonological theory of crime causation was an outcome of this period.

Gradually during medieval period, State started to emerge independent entity by breaking of religious bondages. Marching on the line of secularism, State declared the socio-political and economical sphere as its sole jurisdiction and as crime fall in the list, the definition adopted to treat crime attempted on more secular principles. During this regime scientific and industrial revolution took place rapidly and State started to sponsor activities of venturing for new colonies.

Medieval period had evidenced the eras of renaissance and restoration, which delivered new, and a fresh look to 'crime'. The concepts like utilitarian, positive approach, analytical thinking, principles of natural justice, and thoughts of *lessie faire*, hedonistic philosophy, and pain and pleasure theory were outcome of this period which helped to open new horizons for the study of crime. Latter period paved the way for scientific & industrial revolution and rational way of interpretation dominated the thinking.

This was the period when European countries hurled into wars for grabbing colonies in different parts of the globe. Incidentally, the legal systems of various nations of different parts of the world started to merge and influence each other. This was the basic factor for defining 'crime' on more secular line having social and psychological riders. Historio graphical developments of crime reflect addition and deletion of various acts as a crime and non-crime. Depending on the prevailing dominant factors, the list of criminal acts modified. During this period Indian Criminal System shaped by Britishers on colonial footings.

This process lasted long to World War - II when process of colonization not only stopped, but took reverse gear. Asian and African countries started to liberate from the iron pawn of continental countries to shape their own laws on domestic requirement. However, at the same time, neo-globalization process begins and new types of crime started to emerge challenging the age old notion of sovereign and jurisdiction. [12]These trans-national crimes overthrow the possibility of encompassing it within domestic definition. One of such categories of crime which is new in origin, and requires treatment on different footing is Cyber crime. In this related work from journal, magazine, and books will be read and analyzed to give the appropriate direction to the work. From the Literature survey we can find the as follows:- Categories the cyber crime, types of cyber crimeand their iimpact of cyber crime

III. CATEGORIES OF CYBER CRIME.

There are different types of data crime occurs in the internet like, Data alteration, data interception, data stealing etc

A. Data Alteration

Privacy of communications is essential to ensure that data cannot be modified or viewed in transit. Distributed environments bring with them the possibility that a malicious third party can perpetrate a computer crime by tampering with data as it moves between sites [4]. In a data modification attack, an unauthorized party on the network intercepts data in transit and changes parts of that data before retransmitting it. An example of this is changing the dollar amount of a banking transaction from $100 to $10,000. In a replay attack, an entire set of valid data is repeatedly interjected onto the network. An example would be to repeat, one thousand times, a valid $100 bank account transfer transaction.

B. Data Interception

An attacker monitors data streams to or from a target in order to gather information. This attack may be undertaken to gather information to support a later attack or the data collected may be the end goal of the attack. This attack usually involves sniffing network traffic, but may include observing other types of data streams, such as radio. In most varieties of this attack, the attacker is passive and simply observes regular communication, however in some variants the attacker may attempt to initiate the establishment of a data stream or influence the nature of the data transmitted. However, in all variants of this attack, and distinguishing this attack from other data collection methods, the attacker is not the intended recipient of the data stream. Unlike some other data leakage attacks, the attacker is observing explicit data channels (e.g. network traffic) and reading the content. This differs from attacks that collect more qualitative information, such as communication volume, not explicitly communicated via a data stream [3].

C. Data stealing Term

Used to describe when information is illegally copied or taken from a business or other individual. Commonly, this information is user information such as passwords, social security numbers, credit card information, other personal information, or other confidential corporate information. Because this information is illegally obtained, when the individual who stole this information is apprehended, it is likely he or she will be prosecuted to the fullest extent of the law [5].

IV. NETWORK CRIME

A. Network interrupts

'Network interrupts or incompetent managers trying to do the jobs of the people they normally are in charge of. It could be the above alone, or a combination of things. But if Verizon is using the help the children, hindering first responders line then they might be using network problems as an excuse to get the federal government to intervene in the interest of public safety. Of course if the federal government forces these people back to work what is the purpose of unions and strikes anyway [6].

B. Network Interferences

Network interfering with the functioning of a computer Network by inputting, transmitting, damaging,

deleting, deteriorating, altering or suppressing Network data.

V. ACCESS CRIME

A. Virus propagation

Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are examples of malicious software that destroys the system of the victim [8].

B. Unlawful Access

"unlawful Access" is an insider‘s view of the computer cracker underground. The filming took place all across the United States, Holland and Germany. "Unlawful Access" looks at the personalities behind the computers screens and aims to separate the media hype of the 'outlaw hacker' from the reality [7].

VI. RELATED CRIMES

A. Aiding and Abetting Cyber Crimes

There are three elements to most aiding and abetting charges against an individual. The first is that another person committed the crime. Second, the individual being charged had knowledge of the crime or the principals' intent. Third, the individual provided some form of assistance to the principal. An accessory in legal terms is typically defined as a person who assists in the commission of a crime committed by another or others. In most cases, a person charged with aiding and abetting or accessory has knowledge of the crime either before or after its occurrence. A person who is aware of a crime before it occurs, and who gives some form of aid to those committing the crime, is known in legal terms as an "accessory before the fact." He or she may assist through advice, actions, or monetary support. A person who is unaware of the crime before it takes place, but who helps in the aftermath of the crime, is referred to as an "accessory after the fact" [9, 10].

B. COMPUTER-RELATED FORGERY AND FRAUD

Computer forgery and computer-related fraud constitute computer-related offenses.

C. Content-Related Crimes

Cyber sex, unsolicited commercial communications, cyber defamation and cyber threats are included under content-related offenses. The total cost to pay by victims against these attacks is in millions of millions Dollar per year which is a significant amount to change the state of un-developed or under-developed countries to developed countries. [4]

The review also found that consumers are increasingly concerned about their safety online. The Identity Theft Resource Centre, 2019 Consumer Awareness Survey in the US found that 85 percent of respondents expressed concern about the safety of sending information over the Internet, while 69 percent expressed a need for improvement in the protection of the data they submit over websites. One recent report ranked India in 2018 as the fourteenth country in the world hosting phishing websites [13]. Additionally, the booming of call centers in India has generated a niche for cyber criminal activity in harvesting data, the report maintained. Symantec shares the numbers from its first systematic survey carried out on the Indian Net Security scene: The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic. India's home PC owners are the most targeted sector of its 39.7 million Internet users: Over 86 percent of all attacks, mostly via 'bots'

VII. IMPACT OF CYBER CRIME

A. Crime as an malevolence aspect of society

Despite crimeless society is myth, crime is omnipresent phenomenon, and it is non-separable part of social existence, one may get irritate by the question, ***'Why there is too much ado about crime?'***No one can deny that crime is a social phenomenon, it is omnipresent, and there is nothing new in crime as it is one of the characteristic features of the all societies existed so far, may it be civilized or uncivilized, and it is one of the basic instincts of all human behaviour! However, it should bear in mind that the social concern for high crime rate is not because of it's nature, but due to potential disturbance it causes to the society. In addition, some individuals are victims of crime in a more specific sense. The victims of crime may lose anything that has value. Safety, peace, money, and property are perhaps basic values, because they contribute to the satisfaction of many wishes.

B. Impact over Socio-Eco-Political provision

Conceptually, crime is a dynamic and relative phenomenon and subjected to the relative socio-political & economical changes occurring in existing system of society. Therefore, neither all-time suitable comprehensive definition encompassing all aspects of ‘crime’ is possible at any moment of time nor can a single definition be made applicable to different society. With its dynamicity, it is influenced by the changes occurring in the correlated phenomenon and value system generated by these changes. Incidentally economic crime is on its peak.[24]. This clearly reflects that crime has its interdependency with other social phenomenon, economic systems and political machineries. Also, the population is one of the important factors influencing incidences of crimes. A positive correlation between the growth in incidences of crime and the population of the country has been observed. Besides population, the other factors influencing the crime are such as situation at a particular place, rate of urbanization, migration of population from neighbouring places, unemployment, income inequality, [8]computer literacy in case of Cyber crime] etc.2 At the same time, the economic structure of give society is also influence the economic crimes. As every controlling systems for crime has much to do with the political system which prescribe norms, make rules, create preventive measure, the political structure and system also influence the crime in given society. This clearly demonstrates that every definition of crime has correlation with the socio-economical and political factors.

C. Impact over teenager

These days a worst fear in teenager’s eyes is Cyber Bullying. It is become common over past five years,

generally from the age below eighteen are more susceptible and feared from Cyber Bullying as per inspection . It is becoming an alarming trend in our society. As per inspection of data, the worst fear of cyber crime is on teenagers female. Cyber Bullying is a fear when person receives threats, negative comments or negative pictures or comments from other person. This is all done through core technologies described above mainly via online. Cyber Bullying can be done through chatting, instant messaging etc. Where website like Facebook , Orkut , Twitter user are more affected from Cyber Bullying . In my analysis generally feared person can reach a limit of depression, humiliation and threatens. Through this analysis we come to analyze that if person Bulled online he or she may be depressed up to the level of self harming.

D. Impact of Cyber crime over Private Industry

According the report "Second Annual Cost of Cyber Crime Study – Benchmark Study of U.S. Companies" published by the Penmen Institute, a study is based on a representative sample of 50 larger-sized organizations in various industry sectors, despite the high level of awareness of the cyber threat the impact of cyber crime has serious financial consequences for businesses and government institutions. The report shows that the median annualized cost of cyber crime for 50 organizations is $5.9 million per year, with a range of $1.5 million to $36.5 million each year per company.[26] The total cost is increased if compared to the first study of the previous year. The majority cyber attacks generally refer to criminal activity conducted via the Internet that include cyber espionage, confiscating online bank accounts, creating and distributing viruses to infect the victims, posting confidential business information on the Internet and disrupting a country's critical national infrastructure.

The following chart demonstrate that virtually all companies experienced attacks moved using malware, very interesting also the data related to the action made by the insider and the damages caused by social engineering attacks. The conclusion is that industries fall victim to cyber crime, but to different degrees and with different economic impact. Defense, utilities and energy, and financial service companies experience higher costs than organizations in retail, hospitality and consumer products. [9]The data provided give a clear situation regarding the impact of the cyber crime on the business of large size companies, however a significant impact is observed on the small business where the companies face the cyber threats with fewer resources and accepting the risks related to exposure. In this market segment cyber crime is very fierce and daily it tries to elude helpless companies that often fail to meet the cyber threat, the related damages are devastating causing in many situations the end of the business. In this sector is desirable for governments to support small businesses in harmony with a cyber strategy defined at the national level. Leave helpless the social fabric made up of small businesses has definitely a direct impact also on the business of large firms.

E. Impact of Cyber crime over digital economy

The global reach of the Internet has provided criminals with new opportunities to commit 'traditional' crimes (such as fraud) as well as high-tech crimes that did not exist until relatively recently (such as hacking). Cyber crime and other forms of malicious cyber activity represent a serious threat to the long-term prosperity of Australia's digital economy. Cyber crime is a rapidly evolving phenomenon, with the exponential growth in the global digital economy providing enormous incentives to organised criminal groups to develop cyber crime capabilities.Confidence in e-commerce is also impacted by online consumer fraud, including scams purporting to represent genuine opportunities for businesses and consumers. These activities inhibit consumers' confidence to trade online with legitimate businesses and engage with digital technologies generally.While financial loss is the most obvious impact, other effects can include shame, self-blame and ongoing emotional distress. [10]This work includes undertaking a feasibility study on the establishment of a national online reporting facility, developing protocols to improve cooperation between law enforcement agencies on cyber crime investigation and considering the need for a national approach on cyber crime education and prevention strategies. Recognizing cyber crime's transnational nature, the government is therefore pursuing its intention, announced in April 2010, to accede to the Council of Europe Convention on Cyber crime. The government aims to be a Party to the Convention by the first quarter of 2012.

F. Impact over consumer behavior

The information revolution, coupled with the strategic leveraging of the Internet, has exposed a number of relatively open societies to the dangers of cyber criminal and cyber terrorist acts, especially in commercial business transactions. With the development of e-commerce, this commercial dark side has become known as cyber crime and has taken on many forms that affect the perceptions of the way we shop online.[19] Corporations should realize that these threats to their online businesses have strategic implications to their business future and take proper measures to ensure that these threats are eliminated or significantly reduced so that consumer confidence in the Internet as an alternative means of shopping is maintained. These counter measures, coined as cyber security, have been developed to ensure the safety of consumer privacy and information and allow for a carefree shopping experience. There is need for the development of models that will allow corporations to study the effects of cyber crime on online consumer confidence and to counter through leveraging the benefits associated with the latest developments in cyber security. With these two facets of e-commerce impacting the online consumer, corporations must ensure that the security measures taken will ultimately prevail to assure that consumers will continue to use the Internet to satisfy their shopping needs.

G. Impact over emotion

The first study to examine the emotional impact of cybercrime, it shows that victims' strongest reactions are feeling angry (58%), annoyed (51%) and cheated (40%), and in many cases, they blame themselves for being attacked. Only 3% don't think it will happen to them, and nearly 80% do not expect cyber criminals to be brought to justice— resulting in an ironic reluctance to take action and a sense of helplessness."We accept cyber crime because of a 'learned helplessness'," said Joseph LaBrie, PhD, associate professor of psychology at Loyola Marymount University. "It's like getting ripped off at a garage – if you don't know enough about cars, you don't argue with the mechanic.

People just accept a situation, even if it feels bad."Despite the emotional burden, the universal threat, and incidents of cybercrime, people still aren't changing their behaviours - with only half (51%) of adults saying they would change their behaviour if they became a victim The "human impact" aspect of the report delves further into the little crimes or white lies consumers perpetrate against friends, family, loved ones and businesses. Nearly half of respondents think it's legal to download a single music track, album or movie without paying. Twenty-four percent believe it's legal or perfectly okay to secretly view someone else's e-mails or browser history. Some of these behaviours, such as downloading files, open people up to additional security threats.

H. Impact over business

According to the FBI and the Department of Justice, cyber-crime is on the rise among American businesses, and it is costing them dearly. Cyber-crime includes a myriad of devious criminal practices designed to breach a company's computer security. The purpose of the electronic break and enter can be to steal the financial information of the business or its customers, to deny service to the company website or to install a virus that monitors a company's online activity in the future. [8]

I. Impact over Youth

Cyber communication is society's newest way to interact. Online social networking websites, text messages and emails provide users with an effective, quick way to communicate with people all over the world. Teens in particular spend hours online every day, on computers or personal electronic devices.Family-rescource.com states that 48 percent of teens believe the Internet improves their friendships. With social networking sites becoming increasingly popular, youth are able to stay connected to real and online friends. Some teens believe cyber connections help them feel confident to be their true selves. Instant messaging programs, used by an estimated 13 million teens, allow conversations with friends to occur in real time.[23]. Online communication tools open the door for friendships with other teens near and far.

VIII. FUTURE PROGRESS IN CYBER CRIME

More organizations will adopt social media as a core aspect of their marketing strategy. They will struggle to balance the need to be active as part of on-line social communities while balancing compliance and litigation risks associated with such activities. Similarly, organizations will have a hard time controlling online social networking activities of their users. Attackers will continue to take advantage of the still-evolving understanding of online social networking safety practices to defraud people and organizations. Security vendors will position their products as solving all these problems Improved Social Engineering Attacks will be the trend for the coming era. Attackers will increasingly make use of social-engineering tactics to bypass technological security controls, fine-tuning their techniques to exploit natural human predispositions. This will bring us closer to merging the line between external and internal threat agents, because social engineering will allow external attackers to quickly gain an internal vantage point despite traditional perimeter security measures.

IX. CONCLUSIONS

Research has shown that no law can be put in place to effectively eradicate the scourge of cybercrime. Attempts have been made locally and internationally, but these laws still have shot comings. What constitutes a crime in a country may not in another, so this has always made it easy for cyber criminals to go free after being caught. The future of the Internet is still up for grabs between criminals and normal users. Fears of a cyber apocalypse still abound, while the potential extent of damage that can be caused by wide scale fraud is nearly unbounded. So Cyber crime is growing threat to our society. Today, for the implementation of effective measures for protecting information requires not only protection of information networks and mechanisms for a model of network security and implementation of a systematic approach or a set of data protection - a complex of interrelated measures, described by the definition of "protected information" Hence we have formulated a mathematical model by using multivariate time series analysis, statically analysis, mathematical modelling of past crime patterns to forecast future crime patterns, then the cyber crime can be prevented up to certain extent based on the forecasted accuracy.

REFERENCES

[1] Almulhem, A. Network forensics: Notions and challenges. in Signal Processing and Information Technology (ISSPIT), 2009 IEEE
International Symposium on. 2009.

[2] A.K.Rauta, Y.S.Rao,H. Saini,T.C.Panda A Probabilistic Approach Using Poisson Process forDetecting the Existence of Unknown Computer Virus in Real Time ‘’The International Journal Of EngineeringAnd Science (IJES) Volume 4 , 6 ,PP.47-51,June – 2015,ISSN (e): 2319 – 1813 ISSN (p):2319 – 1805

[3] CERT, CSO, and U.S.S. Service, Cyber Security Watch Survey. Software Engineering Institute CERT Program at Carnegie Mellon
University and Deloitte. 2011

[4] Jantan, A., et al., A Similarity Model to Estimate Attack Strategy Based on Intentions Analysis for Network Forensics, in Recent Trends inComputer Networks and Distributed Systems Security., Springer Berlin Heidelberg. 2012. p. 336-346.

[5] Richards, James. Transnational Criminal Organizations,Cybercrime, and Money Laundering: A Handbook for LawEnforcement Officers, Auditors, and Financial Investigators. Boca Raton, FL: CRC Press, 1999: Pp. 21-54.
[6] Yerra Shankar Rao "Cyber crime Assement "National Conference on Current Trends in Computing (NCCTC) ISBN No. : 978-3-642-24819-6, 23rd -24th March, 2014 ,Page no10-14.,North Orissa University ,Baripada Orissa
[7] Salifu A. Impact of Internet crime on development. Journal of Financial Crime. 2008; 15(4):432–44.
[8] Kwon O, Wen Y. An empirical study of the factors affecting social network service use. Computers in Human Behavior. 2010; 26(2):254–63.
[9] Randa R. The influence of the cyber-social environment on fear of victimization: Cyber bullying and school. Security Journal. 2013; 26:331–48
[10] Analysis of cybercrime and its impact on private and military sectors, by paganinip on April 23rd, 2012
[11] Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm, Visited: 28/01/2012.
[12] Moitra, S. (2004).Cybercrime: Towards an Assessment of its Nature and Impact. Intl. Journal of Comp & Appl. Crim. Justice. Vol. 28, Issue 2, pp. 105 - 124.