Saudi Journal of Humanities and Social Sciences **ISSN 2415-6256 (Print)**
Scholars Middle East Publishers **ISSN 2415-6248 (Online)**
Dubai, United Arab Emirates
Website: http://scholarsmepub.com/

Cyber Crime: An Important facet for promoting Digital Humanities—A Short Review

P.K. Paul[1], D Chatterjee[2], A Bhuimali[3], Abir Atarthy[4]
[1]FBAS, Indian Institute of Engineering Science and Technology (IIEST), Shibpur- An Institute of National Importance, WB, India.
[2]Vice Chancellor, Seacom Skills University, Bolpur, West Bengal
[3]Vice Chancellor, Raiganj University, Raiganj, West Bengal
[4] Co-Founder, ISOAH Data Securities Private Ltd, Infinity Benchmark, Saltlake, Sector V, Kolkata, India

***Corresponding Author:**
P.K. Paul
Email: prancloud@outlook.com

Abstract: 'Cyber' is an important name in the field of Computer Science, Information Science, Legal studies, Business and Commercial Studies and others. Cyber Law and Crime is a kind of interdisciplinary subject incorporated with IT, Computing and legal Studies. In general sense, cyber law is a kind of law and legal aspects which is mainly deals with cyber space and cyber world. In simply manner, cyber space is includes computers, networks, softwares, data storage devices (like- pen drive, hard disk, USB and others), internet, website, mobile phones and others. Though, the emerging arena of cyber law also fall under the category of ATM and similar devices, due to matching nature of such devices with conventional cyber weapon. This paper is talks about cyber crime , law and its various dimension and specially mention about E Crime and its nature and type with special reference to remedial from such kind of offence.
Keywords: Cyber World, Cyber Crime, E- Crime, Cyber Security, Computer and Information Security, Legal Studies, Interdisciplinary Computing

Introduction

Cyber law is actually nothing but the legal aspects that deals with cyber related matter. Virtually cyber law is a bigger concept than other related domain such as internet crime, computer forensic, computer security and so on. Practically information security is a big domain as like cyber law. E Crime is an important aspect which is close to cyber law. Practically, E Crime is mainly responsible for the emergence of Cyber Law. E Crime is includes all the crime and criminal activities related with electronic world [1], [3], [12]. The use of computer, ATM Machine, mobile phone, E mail, internet, Database, telecom network, telephone, computer network fall under the category of E Crime. E Crime and its periphery is emerging and increasing day by day due to invention and integration of new devices, tools and technologies. E Crime is a big terror and kind of offence. E Crime and its awareness still limited in a country like India, thus many people organization and foundation are getting looser day by day.

Objective

The main aim and objective of this study is includes:-

- To learn about E Crime and its relationship with Cyber law.
- To find out main types of E Crime in the age of Super Computing and Cloud Informatics.
- To find out main facet of each E Crime with special reference to their probable solution.
- To find out the main IT Act and its respective section.
- To draw a conclusion as far as E Crime is concerned.

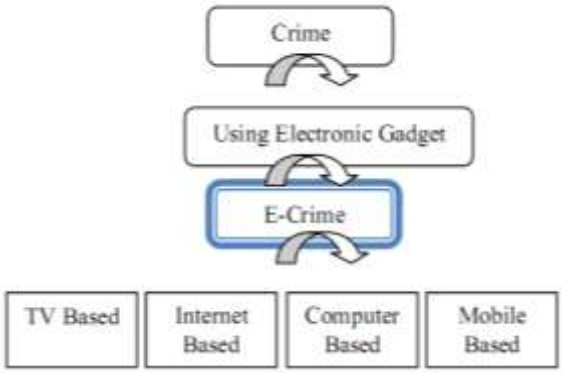

Fig: 1- showing basics of E Crime and its types

E Crime and its types

Information Technology is bring us so many things and application in the field of commerce, business, culture, society, governance, public administration and others activity. Virtually the wider application and utilization of E Crime is also comes with a problem and misuses. This misuse is known as various

nomenclatures, these are- E Crime, Computer Security, Information Security, Network security, Cyber Security, Data Safety, Computer Forensic and others [2].

- E Crime in generally may be classified as various way depending upon weapon we may categories this as TV Based E Crime, Mobile Based E Crime, Internet Based E Crime.
- As far as availability of data, this may be classified as Online Security and Offline Security/Crime.
- Depending upon Computer and Computing, Crime is also possible to classify. The E Crime where computer is directly involved may be called as Computer Crime like- Internet Crime, E Mail Crime, Social Networking Crime, Database Crime, Computer Networking Crime and so on; whereas Computing Crime is indirect computing aided crime where computing and related technologies are just used, these are- ATM Crime, Mobile Crime, TV Crime, Camcorder and Video Crime and so on [5], [12].

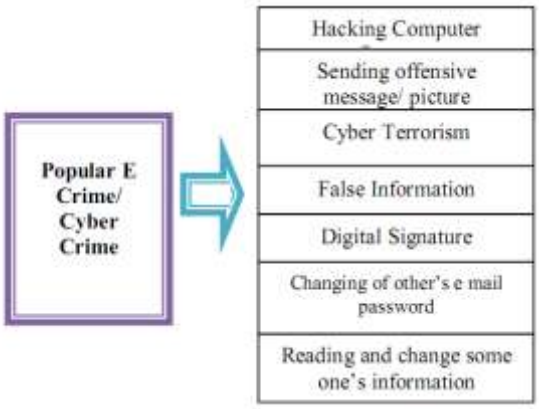

Fig: 2- depicted some popular e crime at a glance

However, out of these, first category of crime is considered as most important and popular. But still most of us is actually not aware about these crimes and its probable solution. Now let look these matter briefly:-

- E Crime and TV: - We may find out E Crime in Television in several way. In most of the cases, some programme are broadcast where anchor inform us that, we need to identify the place or person then they provide us thousand or lakh or prizes. By this way so many people make call and use SMS services and their mobile/ ph account debited a lump some amount as SMS/ call charge beyond normal charges. So without saying actual tariff many viewers debited amount. Like this, many advertisements appear and promise many things and nothing we can get. Some time News channels, Musical and Dance Shows provide interactive part with Mobile or Phone there also charges are hidden in many cases [4], [13].

- E Crime and Internet/ Computer: - Internet based E Crime are most challenges in the field of E Crime and cyber crime. E Crime in internet is normally consider as sending violating or unknown or un expected data, information, audio and video to some one's e mail or any website [6], [7], [12]. But internet and computer based crime may be consider as follows:-

✓ Damaging Computer Documents.
✓ Hacking with Computer Systems, Data alteration.
✓ Sending offensive message through any devices.
✓ Cheating by personal relationship and side by side using computer resources.
✓ Cyber Terrorism.
✓ Publishing or transmitting offensive material in Electronic form.
✓ Publishing false Digital Signature.
✓ False and Duplicate website.
✓ Publishing or transmitting sexual picture or video or fiction; illegal.
✓ Use of children for sexual video or picture and so on.

If we use computer without checking the security system then the whole system may be value less and any attack may be taken place by the attackers. Here attackers may do the crime some of the way like- may only enter the computer by hacking password and only read the information and in second way the attacker enter in the whole computer systems and computer networks and misuse the information [8], [13]. In this category, malware may be implanted in the systems and which is responsible for malfunctions and mischief. In third approach attacker may obtained personally identifiable information from the company's database thus there is a chance for data loss and corrupting financial situation. In 4th approach fear is there for financial data misinterpretation and uses [9], [10]. Think if it is happen in any bank or commercial firm and attackers change the data of any customer's details like- name, details, data or amount and so on. Thus really computer security is very much important in all perspective [11], [13], [15].

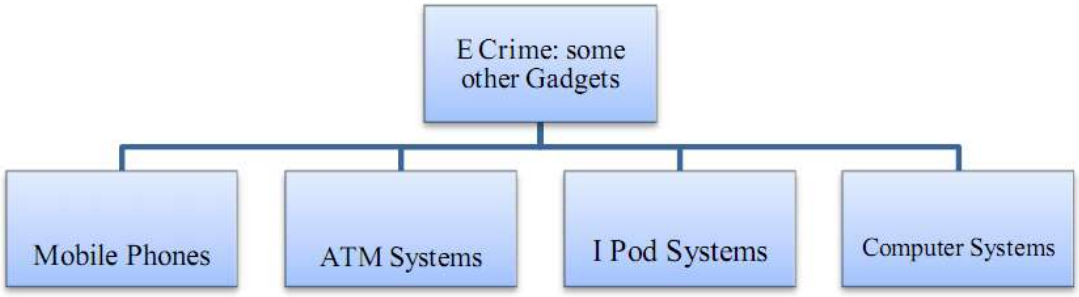

Fig: 3- popular E Crime dealing machines

E Crime and other Gadgets

Apart from internet and television shows other devices related to crime are also increasing. These devises are actually a kind of computing devices but not actually work as conventional computers [12], [19].

Mobile is the most popular device which is now fall under E Crime several way. As like computer, internet is now an important service of a general mobile and thus almost all the problem which are occurred in computer effecting mobile too. Another E Crime is 'False Message' about wining thousand and thousand rupees or dollars or pound and like that. The fraud first get the address then other personal account at the lost they assured new winner can get 1 crore or like that, now they need to send make processing and handling charges of the gift of Rs. 30000 or like that. Winner and fool people send the money and never get the prizes. In some cases, people complaints about mobile service provider for their unsatisfied money deduction. Some time due to hidden condition this may be happen. This is actually may be fall under E Crime [16], [12].

ATM related crime is another one, where fraud and cheater knows user secret password and get the whole money as soon as they have ATM card. In another case, some adhesive or liquid are used on ATM keypad to know secret password and after uses the fraud identify the user's actual password. In third approach ATM details are get the fraud people and they pick their money depending upon need, even time by time. Here user's personal details get through SMS related services and send false message about Banking Formalities [13], [17], [18].

Suggestions

There are several things are possible to do and these are as follows:-

- Computer users need to use very safe password having text and number and that password need to change time to time.
- Virus attack is an important attack in computer thus for data safety antivirus software is essential to use.
- Use of password during some one's presence is need to take care.
- Internet and email security system are essential to choose.
- If it is company or financial data is there, then a strong firewall system is required.
- Regarding TV shows and TV advertisement people can go consumer affairs department or like that As like Use of ATM card of some one's presence is need to be avoid.
- Mobile customers need to follow awareness on wrong and false offers.

Fig: 4- some essentials to secure systems and minimizing E Crime

- If someone threat user orally or by SMS to the mobile then user need to keep the SMS as proof and make FIR at police station, if desired by him/her.

Conclusion

E Crime is increasing and unfortunately side by side the kind or kinds of crime with Electronic gadgets are also emerging. Various software and tools are coming in the market and after certain time later the value of the concerned one is not so healthy. Thus we need to prepare about strong encryption method and firewall system to keep information or data safety. Similarly using some one's photo in a particular place or wrong place is needed to surrender under IT Act and similar cyber law. The legal action may be helpful to reduce this type of crime in certain cases.

Reference

1. Aggarwal, P., Arora, P., & Ghai, R. (2014). Review on Cyber Crime and Security. *International Journal of Research in Engineering and Applied Sciences*, *2*(1), 48-51.
2. Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems*, *36*(1), 93-101.
3. Anwar, Massod, Syed Furqan Qadri, Ahsan Raza Sattar, (2013) "Green Computing and Energy Consumption Issues in the Modern Age", in IOSR Journal of Computer Engineering, 12 (6) Page 91-98.
4. Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448. Catteddu, D. (2010). Cloud Computing: benefits, risks and recommendations for information security. In *Web Application Security*, 17-17.
5. Chowdhury, G (2012) "Building Environmentally Sustainable Information Services: A Green IS Research Agenda" in Journal of American Society of Information Science and Technology, 63(4), Page-633–647.
6. Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*,*43*(7), 125-128.
7. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438-457.
8. Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks*, *57*(10), 2206-2211.
9. Mahara, T. (2013) "PEST- Benefit/Threat Analysis for selection of ERP in Cloud for SMEs", in Asian Journal of Management Research, 3(2), Page 365-373
10. Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2012). Cyber–physical security of a smart grid infrastructure.*Proceedings of the IEEE*, *100*(1), 195-209.
11. Myers KS (Fall 2006). "Wikimmunity: Fitting the Communications Decency Act to Wikipedia". *Harvard Journal of Law & Technology* 20: 163. SSRN 916529
12. Paul, P. K., (2013) *"Cyber Crime and its Challenges with Special Reference to Solution"* in International Journal System Simulation, 7(2), 77-82
13. Paul, P.K., (2013) *"Quantum Information Science-Domain of Future Information Management in Organization and Enterprises: Emerging Interdisciplinary Scenario*" in SIT Journal of Management, 3 (2), 543-551
14. Raysman, Richard, and Peter Brown. *Computer Law: Drafting and Negotiating Forms and Agreements*. Law Journal Press, 1984.
15. Richard Raysman (2009), "Emerging Technologies and the Law: Forms and Analysis", III. Law Journal Press, 2002-2008. ISBN 1-58852-107-9
16. Solove, D.,Schwartz, P.. (2009). Privacy, Information, and Technology. (2nd Ed.). New York, NY: Aspen Publishers. ISBN 978-0-7355-7910-1.
17. Wang, Wenye, and Zhuo Lu. "Cyber security in the Smart Grid: Survey and challenges." *Computer Networks* 57.5 (2013): 1344-1371.
18. Whitman, M. E. (2003). Enemy at the gate: threats to information security.*Communications of the ACM*, *46*(8), 91-95.
19. Zittrain, Jonathan (2003). "Be Careful What You Ask For: Reconciling a Global Internet and Local Law".