IJCSE International Journal of Computer Sciences and Engineering Open Access
Technical Paper Vol.-6, Issue-10, Oct. 2018 E-ISSN: 2347-2693

TECHNOLOGICAL CYBERCRIME IN INDIA AND ITS HINDRANCE

M. Suriakala[1*], P. Narayanasamy[2]

[1]Dept. of Computer Science, Dr.Ambedkar Government Arts College(Autonomous) , Vyasarpadi, Chennai, India
[2]Dept. of Computer Science, Bharathiyar University, Coimbatore, India

Available online at: www.ijcseonline.org

Accepted: 20/Oct/2018, Published: 31/Oct/2018

Abstract- Today new technologies are entering into the world that is providing many informational resources. Technologies are needed in fast moving of information. Maximum security is created, but some lacks in security. It could be identified by cyber criminals and they are moving faster in global era and moreover they could be entering into human privacy. Information is wealth that could bring more facilities to business, entertainment, education and mobility. In India many cyber criminals are rapidly growing and breaking the security to earn money. This could be cultivated day to day by police, but many lacking in software's and investigation. Every day cyber criminals are born and it could be endless one. This paper deals with many security depends on analyzing the various types are crime and deals with methodology like classification techniques to prevent the information from cyber-attacks.

Keywords- Cybercrime statistics, Methods of prevention, Hacking, Unauthorized access and Classification

I. INTRODUCTION

Human being are addicted by many technological software and also observed day to day by technological aspects using computer equipment's, this is the first attach by cyber criminals. Information are enhance every day like government sectors, education, commercial etc., in needed of information most of unknown people using internet without knowing the security level, so that they are entering in illegal website and never studied the terms and agreement. It may cause the major problem for cyber-attacks.Cyber criminals are well trained and technically educated, so that only they break all the security level. In order to solve the problem government should take action and give punishment to attackers. Most of the attack happened on ATM password, money transferring and online purchasing.

Normal human being doesn't know these kinds of cyber-attacks. Most of cyber-attacks happened without having any victims. Many of countries are try to solve many attacks, but lacking and investigation delay only happened. Collection of victims from computers and such electronic device is a big challenge to investigation for officers. Because they find every attacks happens new technological device. According to attacks some governments move to special agencies or officers. In 1820 first cyber-attack place in the cybercrime took place about the Joseph-Marie Jackquard, a textile manufacturer.

II. OBJECTIVE

In this research we can analysis the impact of the cybercrimes by the normal people and how to the government can give the recover from crimes. We try to show what are the safety measures that can do and how can make the maximum security and how to avoid from cyber-attacks.

III. RESEARCH METHODOLOGY

The main is to analysis the secondary data, which is data should collection from various place like government organization. This data can be collected from published data in government website that can be taken into consideration. The data should be more useful for my research. Analysis of historical data we go for classification techniques for making decision support and for prediction. Naïve bayes and J48 can use for decision support for getting accuracy value. It could for future prediction for investigating the raw data. More over association rule is also using for prediction results. My aim is to prevent the people from cyber-attacks and their wealthy information.

Data mining can play the major role in analysis; this could be applied for my research to get prediction data. Some of unpredicted cased can be taken in datamining and find some of predicted results, this could be useful for investigation for future analysis and helpful for human society for maintain peace. Next level of datacanbe preprocessing the huge data that could beprocessedandget clear data set. By cleaning many avoided data can be removed and move on the next processing.

How cybercrime enable?

Some of examples are shown here

a) Junk Mail: junk mails are enabling for money making. It should be unlawful. Many hindranceregulationsare

passed in various countries for unwanted electronic communication.

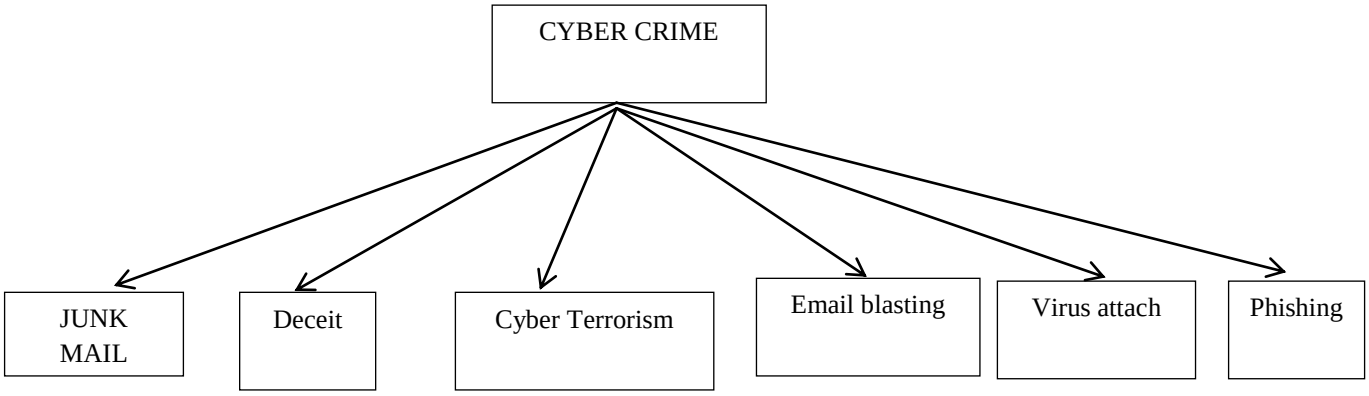
b) Deceit: Newtechnologycomputer device on other side that should hack the information using the computer networks.

c) Terrorism using cybercrime: In order to achieve the politician gains the internet used for terrorism for despoiled the peace [1].

d) Email blasting: This is targeting a person mail or a system. Email bomb threatening the person mail. Sometimes E-bomb crashing the server also.

e) Attaching through virus: A set of instruction send to a person and do malicious operations in the system. It will cause damage to system and person data.

f) Phishing: It mentions to cause damage on stolen passwords and information [2].



Core field diagram and its affected field

Cybercrime Anti - Hindrance methods:

Cybercrime is the most unsafe thread to the developing country. It suffers the developing growth and threatening the citizen for day to day activities. Cybercrime aims the government sectors;non-private organization and private organization arethreatening the activities and earn money. Many of private organization are the most affected one, due to illegal accounts maintenance. Awareness of information sharing that is the main concept for the people; they need the security to defense them. Cyber threads are mostly well trainer in his work. So they do their work without any evidence. They easily migrated anywhere and threatening without any problem [3]. Unknown person in the internet are recorded and they loses their privacy.

Web user are leaving the data without its knowledge, every web user are watching my hidden eye that is cyber thread [4]. Hacking should be done by computer or networks, some ever they sending messages, mail, video etc., to hack the person to cheating them. Here list the severalkinds of perspective electronic crime that are computer crime, internet crime, video or Tv crime and offline [5].

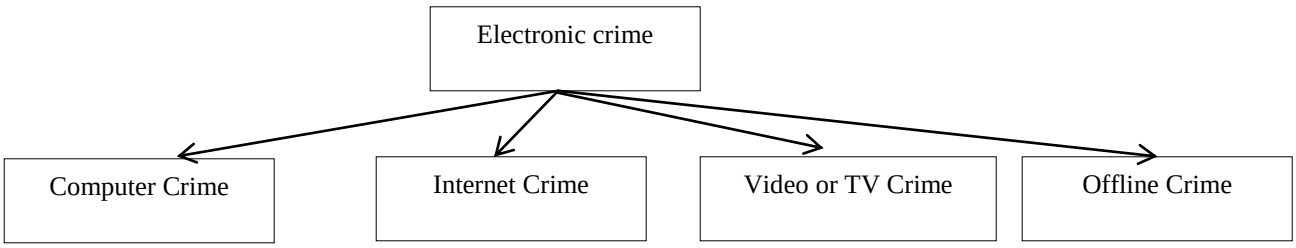


Diagram shows the list for several attacking

Different Types of Characteristics in cybercrime.

They are in silent in nature and affect the privacy and capture the data and play against the citizen life. They are targeting these kinds of people, without having the evidence they threatening the person. It should against the law. They never belong to any country. They are sitting faraway from anywhere and do all economics and privacy crimes. Without your knowledge hidden eye will watching you and observed all data about the persons. They send related mail or advertisement to you to find your data. They watching all those things and make them possible to do crimes against citizen. Especially teenagers are affected mostly belonging to their age. Sometimes big damages against women are done by cybercrime, so it will affect her life [7].

Methods for preventing cybercrime

Many of preventing methods are available on web that can be using them and; it will make ensure to make using of internet. When opening the mail they said to instructed to give password strong, but many of them avoid that, it can be the first entry of cyber-attack to hack mail. So we can use lengthy and using special characters that will make avoiding thread or spam. Don't usesname or related to birthdays or to mobile number, that can be easily find your passwords [6]. First every user know that insert firewall, unnecessary software, open any attachment carefully or in download, use any networks safely, maintain the backup, and finally check security setting using antivirus [8].

Investigation on Cybercrime.

In India many cases are filed against the cybercrime due to development of IT sector. Many new technological devices are invented that could be under the crimes, with this new invention cybercrimes are increasing day to day. So these cases are filed by the government by the ACT of IT 2008 and implemented on amended in 2010. Various cases are filed like data theft, unauthorized person access, virus attack, pornography, cyber terrorism, junk mail, intellectual copy of property etc., Most of cybercrime targeting the business man and National Security [9].

Government punishment and its sections.

Normally when a person involved under the cybercrime they got punishment atthe maximum of 3 years prison or 2 lakhs to fine amount. These are various sections that are given Section 66A- sending unwanted offence message and punishment of 3 years prison and with fine, Section 66B stolen computer assets by receiving and got punishment upto 3 year with fine. Section 66C password, digital signature and other stolen and they got the punishment upto 3 years fine and with fine amount of Rs.1 lakh. Section 66D cheating a person with computer resource, it could be give punishment of 3 year and with 1 lakh fine. Section 66E is Confidentiality or Desecration and got punishment upto 3 years punishment and 2 lakhs fine amount. Section 66F is Cyber terrorism that is offence to national security, if they do have punishment of life time prison. Cyber law refers to the ACT of information technology; the law summarizes the legal issues related to internet [10].

CybercrimeunderClassification:

Datamining has process the large dataset storing in database. Use of datamining we have use tool to convert the data as information. Classification is technique used to prediction value form unknown cases. Mainly classification is used for decision support system. Trees represent the structures with the internal nodes. IFTHEN rules are followed in rule based classifier from the root to leaf, Naïve bayes for probability prediction for cybercrime. So classification is used for future prediction base on the investigation and value should be taken to consideration. Artificial neural network is analytical training techniques that should make new observation using these techniques. More over nearest neighbor Classifier, Support vector machine &Ensemble classifier are the techniques are available to find new decision for any kind of investigation.

IV. CONCLUSION

Cybercrime are harmful to every citizen to the world. Every government are tried to stop this crime, but every electronic discoveryuse beneficiary and sometimes harmful. So every electronic communication should try to make carefully in the internet world. Analyzing every day to day activity we undergo some safety measure and do any type of information communication. Data mining has the future analyze to predict the threatening and its factors. The long tedious process has been used under the data mining tool to get prediction value accurately. The proposed work for the cybercrime is to get optimized results depends upon which technologies have been going to use. This data mining techniques are applied for real world problem in cybercrime and caution the every citizen depends on the analyzing the dataset, which can be occurred by crimes cases using new technical device.

REFERENCES

[1]. S. Shriram, RESEARCH ARTICLE CYBER SECURITY AND RELATED CRIMES IN INDIAN SCENARIO International Journal of Current ResearchVol. 6, Issue, 03, pp.5403-5412, March, 2014

[2]. Shubham Kumar, Guide Faculty - Dr.SantanuKoley, Associate Professor, *Uday Kumar * 2017 "Present scenario of cybercrime in INDIA and its preventions"International Journal of Scientific & Engineering Research, Volume 6, Issue 4, April-2015 1971 ISSN 2229-5518

[3]. AnimeshSarmah, RoshmiSarmah , AmlanJyotiBaruah, "A brief study on Cyber Crime and Cyber Law's of India" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 04 Issue: 06 | June -2017

[4]. Subhash Desai "Study of Online Cyber Crimes in India"American Journal of Computer Science and Engineering SurveyISSN 2349 – 7238

[5]. P. K. Paul* & P. S. Aithal** "cybercrime: challenges, issues, recommendation and suggestion in indian context" International Journal of Advanced Trends in Engineering and Technology (IJATET), ISSN (Online): 2456 - 4664 (www.dvpublication.com) Volume 3, Issue 1, 2018

[6]. 1Alpna, 2Dr. SonaMalhotra "Cyber Crime-Its Types, Analysis and Prevention Techniques" Volume 6, Issue 5, May 2016 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[7]. SoumyaSatishRevankar "cybercrime and cyber security " International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 04 Issue: 11 | Nov -2017

[8]. Jitender Kumar, "Cyber Crime in India: An Overview". Imperial Journal of Interdisciplinary Research (IJIR)Vol-3, Issue-4, 2017ISSN: 2454-1362.

[9]. M. Elavarasi1* and N. M. Elango22017 "Analysis of Cybercrime Investigation Mechanism in India" Indian Journal of Science and Technology, Vol 10(40), DOI: 10.17485/ijst/2017/v10i40/119416, October 2017

[10]. PoojaAggarwal, PiyushArora, Neha, Poonam "Review on cyber crime and security" , 2014International Journal of Research in Engineering and Applied Sciences (IJREAS)

