Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 21 Issue 9, September 2019

Review paper on Cyber Crimes and its Prevention Mechanisms

Dr. Jitendra Kumar Jaiswal
Faculty of Engineering and Technology
Jain (Deemed-to-be University), Ramnagar District, Karnataka - 562112
Email Id: jitendra.jaiswal@jainuniversity.ac.in

Abstract

Cybercrimes are related to criminal activities. The first recorded cyber-crime in the year 1820! It just means there are various digital devices like computers, mobile phones which are used by users through the internet. So, a crime committed by the help of the internet is called a cyber-crime. Cybercrime may target an individual or may be the nation's security and financial health. Information is too important nowadays; information is also wealth and just a way to earn money online. And If this thing is going to be done in an illegal way, happening of cyber-attacks, and data is hijacked from the servers or if money will be filched in an illegal way. So, this review paper describes all about the list of cyber threats happening all over the world up to this time and also prevention mechanisms for that problem.

Keywords: *Cyber Crimes, Hacking, cyber-security, computer Forgery, cyber-attacks, cyber-banking, credit card fraud, cyber security-Internet, cyber-crimes in India, DDoS, Information Technology Act-2000, Mail, Mitigation techniques, Network folders, phishing, Removable devices.*

I. INTRODUCTION

One of the top four economic crimes considered by all organizations has been reported by Cybercrime[1]. According to an Assoc ham report, the number of cybercrimes worldwide will reach a high level of earnings invalid Money Survey data shows how cybercrime is growing at an alarming rate all over the world. What is Cybercrime?Cybercrime defined by the Webopedia "as any type of criminal act done with the help of computers and network (called hacking)" [2]. Cybercrime has a limit targeting illegal digital activities on organizations. The simplest possible definition given for the damage [3]. "Cybercrime is just a crime Some kind of computer or cyber aspect" this definition is given by Norton company. According to Norton gets stolen as someone's identity every 3 seconds consequences of cybercrime[4]. Does not believe in cyber-crime

limitations or regional constraints. Making the cyber world secure is a major concern for all stakeholders. In this regard, every country will have its own cyber law or internet law to control cyber-crimes in your countries. Indian government also formulated a law called the Information Technology Act, 2000 [5]. This act is legal recognition for electronic transactions data interchange and other means of electronic communication and applies across India. Top 5 Crime Chief [5].
The decreasing order is as follows:
Loss or damage to computer resources or utilities
Pornographic publication / broadcast in electronic form
Hacking
Computer source documents tampering
Confidentiality or confidentiality breach
Paper will appear in registered cyber-crimes and one person was arrested on charges of cybercrime. In addition, it describes some cybercrime prevention techniques that have emerged till now. In the final section, cyber threat analysis and its predictions for the coming year are also discussed. The current era is too fast to use the time factor to improve performance. Is only possible due to the use of Internet. The term Internet can be defined as a collection of millions of computers that provide networks and electronic connections between computers. The term cyber-crime can be defined or defined as a law that is left in violation of law or order and for which if convicted, is punished. Other terms refer to cyber-crime as criminal. Activity is directly related to the use of computers, particularly illegal trespassing in computer systems or databases another, the manipulation or theft of stored or on-line data, or the subversion of equipment and data[6]. Internet location or cyberspace is growing very rapidly and in the form of cyber-crimes.

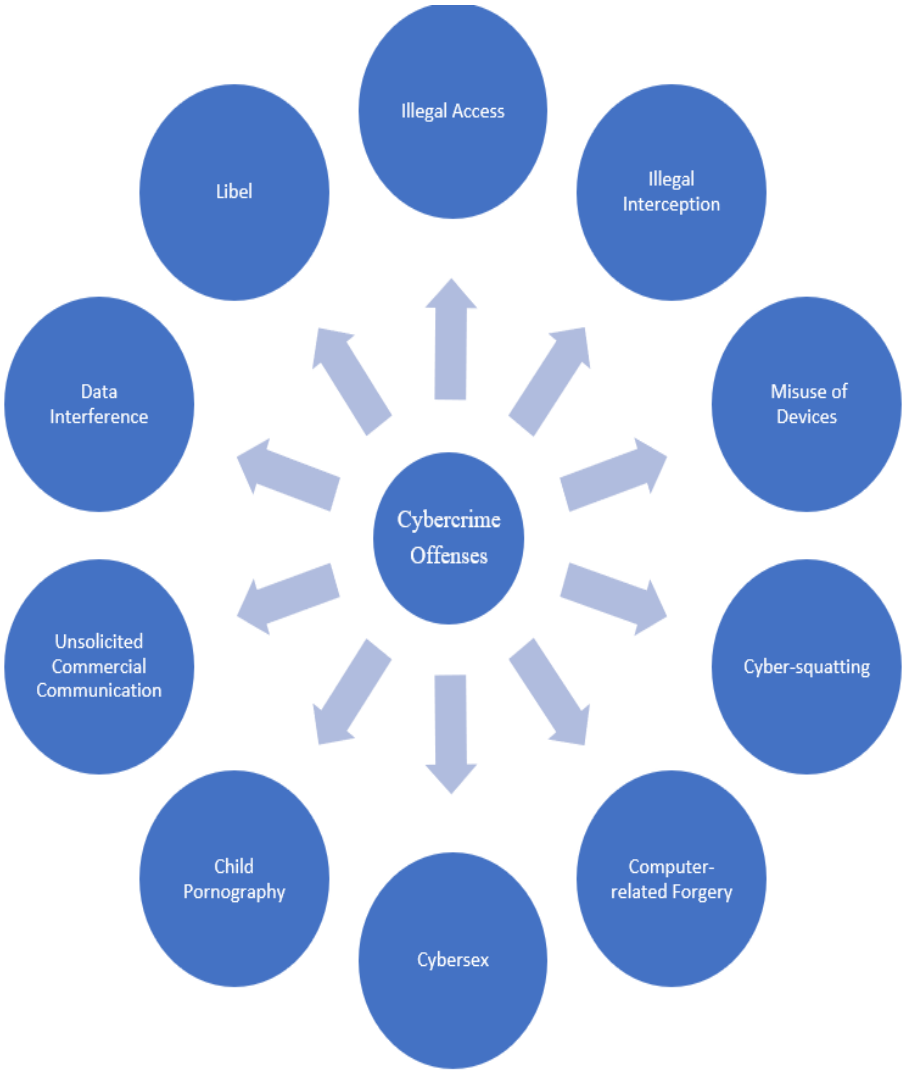

Fig. 1 An Introduction of Cyber Crimes

Cyber-crimes are broadly divided into three major groups such as against crime. And these three groups are:
Individual
Property
Government

A. **Individual:**

These types of cyber-crimes can be in the form of cyber stacking, distributing pornography, trafficking and "grooming". Cyberstalking is the use of the Internet or other electronic means to sting or harass an individual, group or organization. In the present case, law enforcement agencies are considering this type of cyber-crime very seriously and are catching smugglers to join the world.

B. **Property:**

Just as in the real world, a criminal can commit theft and pickup, similarly in the cyber world, criminals' resort to theft and robbery. In this case, they can steal a person's bank statement and withdraw money; Credit card misuse for frequent online shopping; Run a scam for innocent people who have run away from their hard-earned money; Use malicious software to gain access to an organization's website or disrupt the organization's systems. Malicious software can also damage software and hardware, such as damage to barbaric property in the offline world.

C. **Government:**

The crime against the government is known as cyber terrorism. If the culprits are successful, it can create havoc and terror among civilians. In this category, criminals hack or propagate government websites, military websites. The commanders may be terrorist organizations or unfriendly governments of other countries.

Types of Cyber Crimes:

There are various different types of cyber-crimes which are described below.

Cyber Stalking:

It is a type of online harassment, in which the victim is threatened through online messages and emails. Typically, these hunters know their victims and instead of resorting to offline stalking, they use the Internet to stalk them. However, if they notice that cyber stacking does not have the desired effect, they initiate cyber stacking as well as offline stacking to make the lives of the victims worse.

Hacking:

Hacking refers to activities that seek to compromise digital devices such as computers, smartphones, tablets, and even entire networks. And hacking may not always be for malicious purposes, hacking nowadays, and most references to hackers characterize it as illegal activity by cybercriminals - financial gain, protest, information gathering (espionage), and even That "for fun". Of challenge. In this category, a person's computer is broken so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a misdemeanor and punishable. This is different from ethical hacking, which many organizations use to check their Internet security security. In hacking, the perpetrator uses a variety of software to enter a person's computer and the person may not know that their computer is being accessed from a remote location. Many crackers also try to gain access to resources through the use of passwords. Hackers can also see what users do on their computer and can also import files on their computer. A hacker can install many programs on his system without his knowledge.

Malicious Software:

This software, also known as a computer virus, is Internet-based software or programs that are used to disrupt a network. Software is used to gain access to the system to collect sensitive information or data or to damage the software contained in the system.

Computer Vandalism:

It is a type of cyber-crime that damages or destroys data rather than stealing. It transmits the virus.

Software piracy:

It is software piracy through illegal copying of actual programs. Distribution of products to be passed on to origin. If a person with a single user license loads software on a friend's machine, or if a company loads a software package on each employee's machine without purchasing a site license, both the single user and the company compromise the terms of the software license and That's why they are guilty of software theft. Software piracy includes the unauthorized use, duplication, distribution or sale of commercially available software. Software piracy is often labeled as soft lifting, forgery, internet piracy, hard-disk loading, OEM unbundling and unauthorized hiring.

Denial of Service Attacks:

This crime is committed by the perpetrator, which floods the bandwidth of the victim's network or fills their e-mail boxes with spam mail that deprives them of the services they are entitled to access.

Cyber terrorism:

It is the use of Internet based attacks in terrorist activities. Technology savvy terrorists are using 512-bit encryption, which is impossible to decrypt.

Theft:

This type of cyber-crime occurs when a person violates copyright and downloads music, movies, games, and software. There are even peer-sharing websites that encourage software piracy and many of these websites are now being targeted by the FBI. Nowadays, the justice system is addressing this cyber-crime and there are laws that prevent people from downloading illegally.

Identify Theft:

This is a major problem with people using the Internet for cash transactions and banking services. In this cyber-crime, a criminal obtains information about the victim's bank account, credit card, social security, debit card, full name and other sensitive information that returns or purchases money online in the victim's name. Identity thieves can use a person's information to commit fraud to obtain credit, file taxes, or medical services. This can cause major financial losses for the victim and can also disrupt the victim's credit history.

Child Soliciting and Abuse:

This is also a type of cybercrime in which criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms visited by children in order to reduce and prevent child abuse and soliciting.
Virus dissemination: Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, web jacking, e-mail bombing etc.).

Prevention Mechanism

Computer users can adopt various technologies to prevent cyber-crime:
Computer users should use a firewall to protect their computers from hackers. Most security software comes with a firewall. Turn on a firewall that also comes with their router.

Computer users are recommended to purchase and install anti-virus software such as McAfee or Norton Antivirus. AVG provides free antivirus protection, if they do not wish to purchase software. It is recommended by cyber experts that users shop on secure websites only. When investigating, look for a reliable or Verisign seal. They should never disclose their credit card information on a website that looks suspicious or stranger.

Users must develop strong passwords on their accounts, which are difficult to guess. Include both letters and numbers in their passwords. They have to continuously update the password and login details. Changing login details at least once or twice a month reduces the chances of becoming a target of cyber-crime.

It has been suggested how to monitor children and use the Internet. Install parental control software where they can surf.

Ensure that social networking profiles such as Facebook, Twitter, YouTube, MSN are set to private. Check their security settings and be careful about the information that users post online. Once it is on the Internet, it is extremely difficult to remove.

Secure mobile devices. More often than not, people leave their mobile devices inaccessible. By activating the underlying security features, they can avoid any access to personal details. Never keep passwords, PIN numbers and even your address on a mobile device.

Protect data to avoid hackers from criminals. Use encryption for most sensitive files such as tax returns or financial records, do regular back-up of all-important data and store it in a separate location.

Users should be cautious when using public Wi-Fi hotspots. Although these access points are convenient, they are safe. Avoid conducting financial or corporate transactions on these networks.

Protect e-Identity. Users should be careful when giving personal information such as name, address, phone number, or financial information on the Internet. Make sure the websites are secure.

Avoid being scammed: It is suggested that users should assess and consider them before clicking on a link or file of an unknown origin. Do not open any email in the inbox. Check the source of the message. If there is any doubt, verify the source. Never reply to emails asking them to verify the information or to confirm their user ID or password.

In short, cybercrime is developing as a serious threat. A cyber-attack is a computer-generated attack against a website, computer system, or personal computer that compromises the confidentiality, integrity, or availability of information or information stored on it. This is a major and perhaps most complex problem in the cyber domain. Governments, police departments and intelligence units around the world have begun to react against cyber-crime. Many efforts are being done internationally to prevent cyber threats across the border. Indian police have started special cyber cells across the country and started educating people so that they can gain knowledge and protect themselves from such crimes.

II. CYBER CRIMES CASE STUDIES

Below are some of the list of cyber-crimes that happened in the world with full description.

1. ATM System Hacked in Kolkata:

In July 2018, fraudsters broke Canara Bank's ATM server and erased around Rs 20 lakh from various bank accounts. The number of victims was more than 50 and it was believed that they were keeping account details of more than 300 ATM users across India. Hackers used skimming devices at ATMs to steal information from debit card holders, creating a minimum transaction of INR 10,000 and a maximum of 40,000 per account. On 5 August 2018, two people were arrested in New Delhi who were working with an international gang which uses skimming activities to extract details of bank accounts.

Prevention Mechanism:

Promotion of security features in ATM and ATM monitoring systems preventing any misuse of data. There is another way to stop reducing the risk of fraudulent activity using lockbox services to securely receive and transfer funds. It uses an encrypted code that is safer than any other payment.

2. Cyber Attack on Cosmos Bank:

A courageous cyber-attack was carried out in August 2018 cosmos Bank has its Pune branch, which saw about Rs 94 crore. Rupees are being taken away. Hackers wiped out money and It was transferred to a bank which is located in Hong Kong. Hacking the server of Cosmos Bank. Sued by cosmos Bank with pune Cyber Cell for cyber-attack. Hackers hacked bank's ATM server details of multiple Visa and RuPay debit card owners. Attack Cosmos was not on the bank's centralized banking solution. Switching system that acts as an interaction module payment Gateway and Bank's Centralized Banking plow attacked. Malware attack on switch the system has confirmed several incorrect messages that confirm various Visa and RuPay debit card payment demand Internationally. Total transactions were 14,000 in number with over 450 cards in 28 countries[7]. At the national level, this has been done through 400 cards and transactions 2,800 were involved. This was the first malware attack that India broke against the switching system communication between payment gateway and bank.

Prevention Mechanism:

Hardening of security systems by limiting its functions and performance there may be a way forward only for authorized people. Anyone unauthorized access to the network must be set an immediate alarm to block all access to the bank's network. him too reducing risk may enable two-

factor authentication help[8]. Through testing, potential weaknesses can be overcome. Can exclude the entire digital part of the banking system Safe.

3. Hacking the Websites:

Over 22,000 websites were hacked between months April 2017 and January 2018. According to the information Indian computer emergency response is presented by teams on 493 websites affected by malware 114 websites are run by the government. Was intended to gather information about the attack's description of services and users in their network[9].

Prevention Mechanism:

Using more secure firewalls for networks and servers that can block any unauthorized access from outside the network is probably the best idea. Personal information of individuals is important exploitation by users and criminals may not be allowed. Thus, monitoring and launching a proper network, a firewall and security system can help reduce risk of being hacked. These are the most common cyber-crimes so far all over the world. In the upcoming section, using this cyber-crimeis a minor disclosure[8].

4. Blue Security DDOs Attacks:

In 2006 Blue Security was an anti-spam company based in Israel and California. This was an original idea to prevent spam. They will send a request to spammers to stop sending spam every time they used to send spam to their customers. Due to this there were a lot of problems for the spammers. Sending serious capacity issues with Blue Security messages from over 500,000 customers. As far as It was a virtual vigilance system of spamming spammers. Controversially it was clearly quite legal. response from the spammer was attacked by DDoS. Blue security Initially, the attack was responded to in a timely manner. Size and sophistication increased[10]. Blue security had to turn others for support. When Blue Security received Prolexic DDoS security that washed away its traffic from spammers only changed their DDO on Prolexis DNS, which turned them off down and many of his customers who used his service. As a result, Blue Security had to go it alone. Shortly after and as a result the CEO decided to shut down the company.

5. National Australia Bank and Westpac Bank DDoS Attacks:

While Blue Security DDoS attacks will appear Australia, as a tool, has little connivance for DDoS. Australia has seen vengeance many times. In October 2006, National Australia Bank (NAB) issued DDos. Information obtained from law enforcement officers about these attacks were from Russia.

Then in September 2007, Westpac Bank faced an attack with similar traffic patterns after a long time they did not have a new cyber-crime response team established and operated against phishing attacks.

6. Stealing of Credit and Debit card information:

In 2007 three men have been indicted for hacking into cash registers machine at Dave & Buster's restaurant locations in the US stealing data from thousands of credit and debit cards. That data that was later sold and caused more than $600,000 in losses. One from Ukraine and other from Estonia hacked into cash register machines at 11 Dave & Buster's locations and installed "sniffer" programs to steal payment data as it was being transmitted from the point-of-sale terminals to the company's corporate offices. Later the same men were charged with similar a breach at TJMax. Some Analysts estimated the losses at TJ Maxx at more than USD$1 Billion [7]. An inspector with the U.S. Postal Inspection Service alleged one of the three men was a major reseller of stolen credentials [7]. Notably all the three men were arrested while visiting two countries, which actively cooperated with US law enforcement Turkey and Germany and not at home in Eastern Europe.

7. SIM Swap Fraud:

In August 2018, two people from Mumbai were arrested for cyber-crimes. They were involved in fraudulent activities and money transfer related to bank accounts of many people to get information about their sim card by illegal means. These theaters were getting details of people and later their SIM cards were blocked. They were carrying fake documents with the help of the post transactions through online banking. They were accused of effectively transferring 4 crores Indian rupees from various accounts. He also tried to hack the couple's account companies. It will get information about fraudsters customers get their phone number, name, ID proof etc. From an organization or some public domain. After that, they were producing 4G SIM cards. Essential information of customers using 3G SIM card call their phone number and telecom company serves as a customer and customer service executive. They will give a 20-digit number that will be written backwards, ask for a 4G sim card and customer key and activate the 4G SIM card easily. When customers do so, there will be a 3G SIM card will be deactivated and 4G SIM card will be activated. But 4g sim the card is still with the fraudsters in which they will perform banks and receive transactions and OTPs.

Prevention mechanism:

Personal sharing Information can help with unknown applications and domains reduce the risk of having your personal information reaching people with malicious content. Use fraudsters victim

information and victims in various scams deceptive activities[8]. It is recommended that the site where someone is entering their banking or other details must be verified for authenticity, as scammers use fake sites to get information directly from potential victims. In addition, customers are required to activate the SIM card if Physically, they have a SIM card.

III.CONCLUSION

Thus, cyber-crime activities will not stop the next day. Therefore, a better approach is building a powerful system to stop this cyber-crime. Such crimes can be prevented by involving the powerful must have firewall, IDS, SDN controller and maintenance is done periodically. In addition, protecting customer data should be given high priority and should be kept confidential high Secrecy. This is the conclusion of this literature review data is so important that it can be used to earn a lot of money. This manuscript not only looked at the understanding of cyber-crimes, but also explained its implications. Different levels of society. This will help the community to make all online information important. Organizations that are not protected due to cyber-crimes. Understanding the behavior of cyber criminals and the impact of cyber-crimes on society will help in finding adequate means to overcome the situation. The methods to eliminate these crimes can be broadly classified into three categories: Cyber law (known as cyber Law), education and policy making. All the above methods for dealing with cyber-crimes are either very less. Many countries do not have significant work or anything. This lack of work requires improvement in existing work or establishing new paradigms to control cyber-attacks.

IV. REFERENCES

[1] World Economic Forum, The Global Risks Report 2017 12th Edition. 2017.
[2] A. Al Mazari, A. H. Anjariny, S. A. Habib, and E. Nyakwende, “Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies,” in Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, 2018.
[3] E. Kitchen, “US Cybercrime: Rising Key findings from the 2014 US State of Cybercrime Survey,” Natl. Serv. Secur., 2015.
[4] Techopedia, “What is Cybercrime? - Definition from Techopedia,” Techopedia, 2018. .
[5] P. N. V. Kumar, “Growing cyber crimes in India: A survey,” 2016, doi: 10.1109/SAPIENCE.2016.7684146.
[6] Z. Guo and Y. Guan, “Active probing-based schemes and data analytics for investigating malicious fast-flux web-cloaking based domains,” 2018, doi: 10.1109/ICCCN.2018.8487410.
[7] P. Warren, K. Kaivanto, and D. Prince, “Could a cyber attack cause a systemic impact in the financial sector?,” Bank Engl. Q. Bull., 2018.
[8] S. C. N.-H. 3. I. D. 2018 Devi, National security in the digital age: a study of cyber security

challenges in India. 2018.

[9] H. Berger and A. Jones, “Cyber security & ethical hacking for SMEs,” 2016, doi: 10.1145/2925995.2926016.

[10] R. (200. R. from http://www. sciencedirect. com/science/article/pii/S0169555X1200381. Carley, J., Pasternack, G., Wyrick, J., & Barker, J. (2012). Significant decadal channel change 58–67years post-dam accounting for uncertainty in topographic change detection between contour maps and point cloud models. Geomorphology, Caballero, Y., Cheva et al., “RESTORING THE FISH FAUNA CONNECTIVITY OF THE HÂRTIBACIU RIVER-RETIŞ DAM STUDY CASE (TRANSYLVANIA, ROMANIA).,” Acta Oecologica, 2017.