ISSN: 0974-5823 Vol. 7 No. 6 June, 2022

International Journal of Mechanical Engineering

CYBER CRIMES IN INDIA: A CRITICAL ANALYSIS

Rani Supriya
Law College Dehradun, Uttaranchal University,Dehradun-248007, Uttarakhand, India.

Km. Pranjali Tomar
Law College Dehradun, Uttaranchal University, Dehradun-248007, Uttarakhand, India

Kuljit Singh
Assistant Professor, Law College Dehradun, Uttaranchal University, Dehradun-248007, Uttarakhand, India.

Mr. Manish Bhardwaj
Assistant Professor, Law College Dehradun, Uttaranchal University, Dehradun-248007, Uttarakhand, India

Mr. Shashank Tyagi
Assistant Professor, Law College Dehradun, Uttaranchal University, Dehradun-248007, Uttarakhand, India

ABSTRACT

As a result of the COVID- 19 pandemic, the world has moved to digital channels, resulting in a surge in cybercrime. India experienced an 86 percent rise in cyber-attacks from March to April, 2020. Because, the Internet has no geographical limits and the face of cybercrime is still unknown, cybercrime is on the rise. With the widespread use of information and communication technology in India, cybercrime is increasing day by day. People have become reliant on the internet for all of their requirements as technology has advanced and the internet allows them to access everything.

Online studies, online jobs, online shopping, financial transactions, and requirements of a man's life can now be fulfilled over the internet. With the growth of the internet, different kinds of cybercrime have emerged. This article explores an overview of cybercrime and its evolution. We would also like to discuss the different types of cybercrime that people are currently facing and the unique challenges and problems that can be faced, prevented and resolved (if possible).

Keywords: Cybercrimes, Internet, Computers, Cyber stacking, Hackers.

1. INTRODUCTION

India has the second-highest client-based internet in the world in its emerging digital economy. (Singh & Loura, 2021).Illegal activities on computers are referred to as cybercrime. In the new millennium global economy has witnessed a new revolution –the entrance of world from physical world to cyber world. (gagandeep, 2013).Traditional crimes can be performed with or without the use of a computer, however cybercrimes include more particular sorts of crimes like phishing schemes and viruses (22Ma2). Cybercrime, commonly known as "online crimes or computer crimes," is any criminal activity that takes place through the internet. Cybercrime

is a relatively new form of criminal activity in the world. Cybercrime is considered as any criminal activity, that occurs or takes place on or through the use of computers, the internet, or any technology recognized under the Information Technology Act. Cybercrime is the most efficient and widespread crime in India, and it has a bad and devastating impact. Criminals not only cause devastated and long term damages to society, but to the Government also, but they also conceal their identities to a large and substantial extent.

Technically, adept criminals engage in a variety of unlawful activities over the internet. Cybercrime, in a broad sense, refers to any act to include any illicit activity involving a computer or the Internet as a tool or target, or both (22Ma3) .

Although the term "cybercrime" has been defined in some Indian court judgment, it has yet to be defined in any law or statute passed by the legislature of India. Cybercrime is an unstoppable evil based on the misappropriation of modern society's growing reliance on technology. Computers and other related technologies are becoming more prevalent in daily life, and they have become a much-desired convenience for users (Vakul Sharma, 2011). It is an unfathomable and endless medium. Whatever positive effects the internet has on us, it also has negative effects. Cyber terrorism, email spoofing, email bombing, cyber content, and cyber sabotage are examples of emerging cybercriminals. Some ordinary crimes can be classified as cybercrime, if they are carried out through the Internet .

2. ORIGIN OF CYBER CRIMES

Although the term "cybercrime" has been defined in some Indian court rulings, no legislation or statutes passed by Indian legislature defines it. Cybercrime is an unstoppable evil based on the misappropriation of modern society's increasing reliance on technology. Computers and other related technologies are becoming more prevalent in daily life, and they have become a much-desired convenience for users. It is an unfathomable and endless medium. Whatever positive effects the internet has on us, it also has negative effects. Cyber terrorism, email spoofing, email bombing, cyber content, and cyber sabotage are examples of emerging cybercriminals. Some ordinary crimes can be classified as cybercrime, if they are carried out through the Internet network that could function in the times of disaster or war and transmit information securely.

In India, the State-owned entity, that is, “Videsh Sanchar Nigam Limited” introduced internet services in 1995, and the Government abolished the VSNL monopoly in 1998, opening the market to private operators.

In the year 1820, the first recorded cybercrime occurred. It is notable that the abacus, a type of computation, has been used since 3500 B.C. in India, Japan, and China. The analytical engine of Charles Babbage, on the other hand, marked the beginning of the contemporary computer age. The loom was created by Joseph Marie Jacquard, a textile maker in France, around 1820. This technology allowed a succession of steps in the weaving of specific fabrics to be repeated. Employees at Jacquard were concerned that their traditional jobs and livelihood might be jeopardized as a result of this technology. They used sabotage to prevent Jacquard from using the new technology in the future. *This is the first cybercrime to be documented.* In respect of digital crime, there was more focus on legislations in the 1980s as businesses became more and more reliant on computerization and it catalyzed the cases, which are vulnerable and exposed to computer crime.

3. TYPES OF CYBERCRIMES

3.1 Identity Theft

When a thief obtains personal information, they can use it to steal money and gain access to private and sensitive information. They also exploit people's names to set up phony accounts and to carry out illicit acts. Identity theft is a highly widespread crime in today's cyber environment. *According to the Norton Life Lock Report,* nearly four out of ten Indian respondents, or 40%, have been victims of identity theft. A bank management trainee was engaged and about to marry in the BANK NSP CASE (22Ma4). Using the company's computer, the couple exchanged numerous emails. After the pair had broken up for a while, it was discovered that the girl had created a false email account in the name of the Bar Association of India and was sending harassing emails. Text

messages and emails to foreign clients of the boy. Since she is close to the boy, she has all his business and personal information of the boy and all the details of the client that the boy was dealing with. She used the banks computer to send these emails .this resulted in a loss of many clients of the boys company and the company sued the bank. The bank was held responsible for sending sms and emails through its server.

3.2 CYBER STALKING

Professor Lamber Royakkers explains:

A cyber stacker is someone who allegedly harasses others via electronic and internet means for love or sexual reasons. Message boards, chat rooms, emails, spam, faxes, buzzers, and voicemails are all options. Stalking usually entails harassing or intimidating others on a regular basis. Since stalking behaviors are numerous and must be evaluated in their relationship, they include stalking someone, visiting their home or places where they work, harassing calls, leaving text messages or belongings, and vandalizing their property. It is tough to give an accurate description of stalking.(22Ma5)

3.3Phising

Criminals utilise social engineering to get in touch with you directly, usually through phone or email. In order to gain your trust and collect the information they require, they usually act as a customer service representative. Your passwords, your employer's name, or your bank account number are examples of this information. Before attempting to add you as a friend on social media networks, cybercriminals will acquire as much information about you as possible on the internet. After gaining access to an account, they can sell your information or start accounts in your name.

The goal of phishing is to trick people into revealing their credit card numbers, passwords, bank account numbers, and other personal information with a legitimate company when, in reality, they are exchanging their information with a fraudulent website or organisation that will steal their money.

3.4 Data Theft

Data theft is a type of cybercrime in which fraudsters or hackers get unauthorized access to sensitive and private information that is not intended to be disclosed publicly. In other words, it refers to the theft of information that is then exploited unethically, bringing harm to large corporations. By taking someone's identity, address, and position, one such occurrence can bring down a large organisation. One instance of employee data theft not only traps that individual, but also has an impact on the company's general reputation and existence**.**

3.5 Data Diddling

Modifying data before or during entry into a computer is known as data diddling. To put it another way, information is altered by a person putting in the data, a virus changing data, a database or application programmer changing data, or any other person participating in the saving process of information saved in a computer file. Anyone participating in the recording, encoding, reviewing, checking, transforming, or transmitting of data can be the perpetrator. Although committing a crime is simple, the consequences can be costly.

In India, power firms are disproportionately affected by this type of criminality. The NDMC Electricity Billing Fraud Case in 1996 is an excellent example. The NDMC, Delhi, used the computer network to receive and account for electrical bills. A private contractor who was a computer specialist was solely responsible for cash collection, computerized bookkeeping, record keeping, and bank remittance. He misused a large sum of money by altering data files to represent fewer receipts and bank transfers.

3.6 Domain Name violations and passing off

A domain name is an address for a computer or device connected to the internet. Domain names now serve as trade names or trademarks and carry the goodwill and reputation of websites, thanks to the progress of internet communication and the growth of e-commerce and its future possibilities. Since e-commerce was done in the absence of physical interaction or the possibility to check the items, domain names have gained prominence and legal sanctity as a means of distinguishing amongst e-players .

In the case of Card service International Inc. v. M.C. Gee, it is assumed that a domain name serves the same purpose as a trademark and is not just an address or a number of internet searches, and hence is entitled to the same level of protection as a trademark. A domain name is also regarded to be more than just an online address, because it also identifies the internet website and individuals, who visit it, just like a person's name does .

3.7SoftwarePiracy

The act of stealing legally protected software is known as software piracy. Theft of software includes copying, distributing, changing, or selling it. Software piracy does not necessitate the use of a hacker or professional programmer. If they are unaware of the software laws, any ordinary person with a computer can become a software pirate. Because of its pervasive impact, it's critical to comprehend what software piracy is and the risks it poses.

.The Copyright Act of 1957 oversees computer software in India. In 1995, Congress modified the Copyright Act of 1957 to keep up with improvements in science and technology, particularly, in the fields of communication and computer processing. 'Computer Program' is defined as a literary work in Section 2(ffc) of the Copyright Act **.**

3.8 SMS SPOOFING

SMS spoofing is similar to e-mail spoofing, it appears to originate from a known number that belongs to you, but it is actually spoofed and sent by a hostile individual. Consider the following scenario. Consider a lady, who receives a text message from her husband's phone in the middle of the night, instructing her to bring cash because he has been in an accident. She'll almost certainly check the phone number, and if it's her husband's, she'll hurry out with cash. If this is her reaction, she is most likely unaware of the term "Mobile Spoofing." A cybercriminal might send a message from anyone’s phone using web based software without ever touching that person’s phone, and no cellular service provider could tell it was spoofed or fabricated (22Ma6).In Sms Spoofing, a person replaces the original mobile number(sender id)with alphanumeric text, when that person sends the spoofed text.

4. CYBER LAWS

As the present universe is surrounded by the power of new mantra name “Information technology”. With the appearance of the IT Act most of the countries have switched over to paper based governance to e-governance**.**(gagandeep, 2013)**.**

4.1 Laws related to Cybercrime under the IT ACT, 2008.(The Information Technology (Amendment) Act, , 2008)

Sec. 65: It is related to tampering with computer source and documents. Any person who knowingly or intentionally conceals, destroys or alters any computer system and the punishment for this offence is for the term of 3 years of jail and fine would be for up to 2lakh rupees, or both.

Sec.66: It elaborates about hacking of computer system and tampering with data and computer. Any person who does a dishonest and fraudulent act which is mentioned and explained under Sec. 43 of this Act and the punishment for this offence is for the term of 3 years of jail and fine would be for the amount, which may not go beyond 5 lakh rupees, or both.

Sec. 66A: It explains the punishment and penalty for transmitting offensive texts, which includes up to three years in prison and fine. The term electronic mail refers to the message or information transmitted on computer resource or communication device including any attachment in text images, audio, video or any other electronic records that may be transmitted with messages.

Sec.66B: It elaborates about the punishment and penalty for dishonestly receiving stolen computers resources or communication equipment, whoever dishonestly receives any stolen computer resource or having reason to believe that the computer resource is stolen. The punishment for that is imprisonment up to 3 years, and fine up to 1 lakh, or both.

Sec.66C: It elaborates about the punishment and penalty for identity theft, whoever makes dishonest use of any other person's electronic sign and password or other unique identification feature and retribution. The punishment is for a term of sentence up to 3 years and fine would be for the amount, which may not exceed from1 lakh rupees.

Sec.66D:It explains that whoever cheat by personating using any communication device or computer and retribution, The punishment is for a term of sentence up to 3years and that person will be fined, which may not exceed above 1 lakh rupees.

Sec.66E: It explains that a person, who intentionally records, publishes, an image of person's without his or her consent, in circumstances that violate that person's privacy and retribution. That person would be sentenced up to a term of 3 years and will be fined for the amount, which may not exceed2 lakh rupees or with both the term of sentence and amount of fine.

Sec.66F: It elaborates about the charge and retribution, which means penalty or fine for cyber terrorism, retribution. An offender would be sentenced for whole life.

Sec.67: It elaborates that whoever publisher ,transmit or cause to be published in electronic form any material, that is lascivious or appeals to the prurient interest, or whose effect is such as to tend to deprave and corrupt persons, who are likely ,in light of all related circumstances, to read, see or hear the matter contained in it and penalty upon first conviction, the person will be sentenced for a term of three years, and will be fined for the amount up to 5 lakh rupees, and upon second conviction person will be sentenced for up to *5* years and will fined for the amount up to 10 lakh rupees.

Sec.68: It elaborates about the direction of the controller, and the person, who would be caught committing that crime, would be sentenced with up to*2* years and will be fined for the amount up to 1 lakh rupees or with both with the term of sentence and amount of fine.

Sec.69: It elaborates about power to give instructions or orders for interception, monitoring or decryption of information from any computer resources, and person will be sentenced for the term up to *7* years and will be fined.

Sec.69A: It elaborates about the authority to give orders for prohibiting the public access of any information via any computer resources, and an offender would be sentenced for a termup to *7* years and will be fined.

Sec.70; It elaborates about entry into a protected or secured system, without authorization, and person will be sentenced for the term up to 10 years and will be fined with the amount.

Sec.70A: It elaborates about "National Nodal Agency", and an offender would be sentenced up *to 10* years and or with the amount of fine.

*Sec.70B:*It elaborates that "ICERT in to serve as national agency for incident response. Violating the directions of Indian computer emergency response team", and the authority responsible for it, will be sentenced for a term up to one year and will be fined with 1 lakh rupees or both, with the term of sentence and amount of fine.

Sec.71: It applies to any person, who intentionally misrepresents information or withholds material facts from controller or certifying authority in order to obtain a license or electronic signature certificate, and the person will be sentenced for the term up to 2 years or will be fined for the amount of1lakh rupees or both, with the term of sentence and amount of fine.

Sec.72: It elaborates about the invasion of privacy and confidentiality, and the person will be charged with the sentence of up to *2* years or will be fined with amount of up to 1 lakh rupees or both, with the term of sentence and amount of fine.

Sec.72A: It elaborates about charge for information disclosure in violation of lawful contract, and an offender will be sentenced for up to *3* years ,or will be fined for the amount up to 5 lakh rupees, or both, with the term of sentence and the amount of fine.

Sec.73: It would apply to a person, who publishes or makes available an electronic signature certificate knowing that the certifying authority hasn't issued it, the subscriber hasn't accepted it, or the certificate has been cancelled or suspended, and that person would be sentenced with a term up *to 2* years or will be fined for the amount of up *to 1* lakh rupees or with both, the term of sentence and amount of fine.

*Sec.74:*It elaborates that a person, who knowingly generates, publishes or otherwise makes available an electronic signature certificate for any fraudulent or unlawful purpose, and person will be sentenced for the term up to *2* years or will be fined for amount up *to 1* lakh rupees or with both, the term of sentence and amount of fine.

4.2 CYBER CRIMES UNDER THE IPC, 1860(The Indian Penal code, 1860)

- *Sec. 292*:This section is to address, the sale of obscene materials, it has developed to include different cybercrimes in the digital age. This provision also governs the electronic publication and transmission of obscene material, sexually explicit activities, exploit acts involving children, and so on. Though the offences listed above appear to be similar, the IT Act and IPC recognize them as distinct offences. The penalty for committing such activities is sentence which may not exceed the two years and an offender will be fined for Rs. 2000. This crime, has been committed repeatedly for the second time, then, the offender will be sentenced for a term, which may exceed to *5* years and will be fined for an amount not exceeding Rs. 5000. (22Ma7)

- *Sec. 419 and Sec. 420*:The provisions of these Sections are clubbed together, since these Sections deal with fraud. These two sections of the IPC deal extensively with crimes, such as, theft of password for the reason of gaining fraudulent reasons, the construction of phony websites, and the committing of cyber scams. Email phishing, on the other hand, is only related with Section 419 of the IPC, because it consist of assuming identity of someone, and demanding a password. Section 419 has a retribution, an offender will be sentenced up to 3 years or will be fined for an amount, while Section 420 carries a retribution, where sentence is up *to 7* year or fine. (22Ma8)

- *Sec. 465*:The penalty for forgery is addressed in this section. Offenses such as email spoofing and the creation of fake papers in cyberspace are dealing with and punishment is given under this Section, which carries the sentence up to 2 years or fine or both. "In *Anil Kumar Srivastava v. MHFW,* (K.A, Indian Penal Code, 2017), the petitioner electronically forged the signature of the AD and then filed a lawsuit alleging false allegations against the same individual. The petitioner was found liable under both Section 465 and Section 471 of the IPC, because he attempted to pass it off as a legitimate document."

- *Sec. 499*: It dealt with defamation,(22Ma9) sending defamatory messages by email. Defamation occurs when someone makes or publishes a false or misleading remark, allegation, or imputation about another person, whether through words, oral communication, signs, or any other means. In case of *D.P. Chaudhary*

& ors v. Kumari Manjulata, (DP Chaudhary&ors v. Kumari Manjulata, 1997), the defendant is accountable, if he has the desire to harm or cause injury to the plaintiff's reputation, but he had no such intention and no such purpose in mind, when he penned those remarks. Every person must assume that he is aware of the implication of his action. Even if the words were mistakenly published, they are actionable, if they are false and defamatory.(22Ma10)

- *Sec.500*: It talks about email abuse. In terms of cybercrime, Section 500 of the IPC will be used to prosecute anyone, who sends defamatory or abusive messages over email. This section carries a maximum sentence of two years in prison and fine. (K.A, Indian Penal Code, 2017)
- *Sec.504*:It talks about sending threatening messages by email. Threatening, insulting, or attempting to instigate another person with the goal of bringing about peace through email or any other electronic form is a violation of Section 504 of the IPC. This violation carries a penalty of up to two years in prison, a fine, or both. (K.A, Indian Penal Code, 2017)
- *Sec. 506*: It elaborates that if a person tries to criminally threaten another person, over a person's life, property destruction through fire, or a woman's chastity, that person will be charged under Section 506 of the IPC, which carries a maximum sentence of seven years and will be fined, or both. (K.A, indian Penal Code, 2017)
- *Sec. 509*: It deals with the offences of saying something, making a gesture, or doing something that could impair a woman's modesty. It also includes voice made and action committed that disturbs the privacy of any female. If this offence is committed physically or electronically, Section 509 is invoked, and the retribution, which may not exceed to sentence of 1yearor amount of fine, or both. (K.D, 2016)

5.ANALYSIS OF CYBER CRIMES IN INDIA

According to the latest data from National Crime Record Bureau (NCRB), a total of 27,248 cases of cybercrimes were registered in India (22Ap).

Total number of cyber-crimes reported in India from 2012-2021

2021	68,045
2020	50,035
2019	44,735
2018	27,248
2017	21,796
2016	12,317
2015	11,592
2014	9,622
2013	5,693
2012	3,377

From the above table, it is clear that there has been increase in the number of cybercrimes cases in India after the passage of each year. The main kinds of cyber-crimes are fraud, scam, credit card fraud, identity theft scam, online harassment, cyber stalking, cyber bullying, invasion of privacy, etc.

6.CONCLUSION

We live in a digital age, when cyberspace is not limited to one's own bounds, but rather encompasses the entire world .As a result, cybercrime is on the rise in every country, including India. The most difficult part of cybercrime is its dynamic aura, which widen from the continual advancement of digital technology. As a result,

new cybercrime techniques and approaches are developed. As a result, cybercrime should be given the same priority as other forms of crime in our society, such as theft, rape, and murder.

In future, integrity in cyber network of India will be increasingly challenged and fragile. (Singh & Loura, 2021)With the country advancing towards 'Digital India Movement', people are currently living in digital world, where almost thing of a person is going digitally, and as result of it cybercrimes is increasing day by day. The biggest challenge in cybercrime is its dynamic nature, because it has no any specific location or any specific identity. Cyber criminal's real identity is not revealed from the commencement of the crime. So, cybercrime should be given as much importance as other crimes of our society. The current cyber law system is still not so developed and sufficient to prevent the wide scope of cybercrime, which is currently happening around us. Even we have no legislation to deal with the new kind of cybercrime, which is rising from developing technology. The law enforcement authorities, the private corporations and organizations will also have to change their methods to reduce it or to deal with it. Besides, the major point, which needs to keep in mind that the information technology is very wide and dynamic, a culture of continuous and constant cyber education and learning amongst the legal and the law enforcement bodies is sine qua non. The most effective solution or method of overcoming any problem is not to enact a plethora of statutes, but to ensure that they are strictly and dedicatedly enforced. The courts have the authority to cause to implement the existing laws in a progressive and purposeful manner. At last, it can be concluded that the technology should be used for development of society, not for harming and disturbing the members of the society.

7.SUGGESTIONS

The judiciary can only play an important role in cyber law enforcement, if equipped with high technology. It could administer the justice efficiently. E-justice can provide a quick path to conviction of cybercriminals without unreasonable delay. Delay in follow up leads to loss of evidence. It is notable that as compared to other records, electronic records are not permanent.

In order to prevent cybercrimes, there are various measures that a person should know for prevention and controlling of cybercrime by law and public:

1. There is need to develop International Standards of security measures.
2. Netizens must destroy and remove confidential information after using it and they should also use their own ways of communication, such as, secret and confidential fiber methods.
3. There is requirement of regular update of antivirus software, changing the password, updating the operating system.
4. In response to prevent and regulate net warfare, investigating authorities and committees must have the authority to deface terrorist website and networks.
5. To prevent and control cyber terrorism, laws and legislation must be developed accordingly.
6. A person should never disclose their personal information while chatting through several social media platforms or emails.
7. Currently, credit card fraud is very common, so a person should never give their credit cards' details to any fake, forged and unsafe website as the protection against fraud.
8. The misuse of photograph of the persons is increasing and rising day by day, the best measure is to avoid the sharing of any pictures and images to strangers online.

REFRENCES

1. (n.d.). Retrieved May 5, 2022, from https://blog.ipleaders.in/critical-analysis-cybercrime-india
2. (n.d.). Retrieved May 5, 2022, from https://blog.ipleaders.in/critical-analysis-cybercrime-india
3. (n.d.). Retrieved May 10, 2022, from http://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf
4. (n.d.). Retrieved April 11, 2022, from http://www.thehindu.com/tag/611-608-600/cyber-crimes
5. (n.d.). Retrieved May 5, 2022, from https://blog.ipleaders.in/critical-analysis-cybercrime-india
6. (n.d.). Retrieved May 10, 2022, from http://www.sociosite.org/cyberstalking_en.p
7. (n.d.). Retrieved May 10, 2022, from the new phony crime: SMS spoofing, PTI, Jul 11, 2004 http://timesofindia.indiatimes.com/The-new-phony-crime-SMS- spoofing/article show/773923.cms
8. (n.d.). Retrieved May 15, 2022, from https://blog.ipleaders.in/punishments-cyber-crimes-ipc/
9. (n.d.). Retrieved May 15, 2022, from https://blog.ipleaders.in/punishments-cyber-crimes-ipc/
10. (n.d.). Retrieved May 15, 2022, from https://www.legalserviceindia.com/legal/article-8
11. (n.d.). Retrieved May 15, 2022, from https://www.legalserviceindia.com/legal/article-8011-defamation-in-ipc.ht
12. Manish Kathuria v.Ritu kohli, 14616 (High Court of Punjab,Chandigarh 2014).
13. (1860). In *The Indian Penal code.*
14. (1860). In *The Indian Penal code.*
15. (2008). In *The Information Technology (Amendment) Act, .*
16. (2021). *Crimes of India, Report on Cybercrime.* National Crime Record Bureau.
17. DP Chaudhary&ors v. Kumari Manjulata, 170 (Rajsthan High Court 1997).
18. Gagandeep, K. (2013). Consumers in E -Commerce : A New Challenge for Consumer Protection Jurisprudence in India.Dehradun Law Review, *5*(1), 45-50.
19. K.A, P. (2017). *Indian Penal Code.* Lucknow: Eastern Book Company.
20. K.A, P. (2017). *Indian Penal Code* (4 ed.). Lucknow: Eastern Book Company.
21. K.A, P. (2017). *Indian Penal Code* (4 ed.). lucknow: Eastern book company.
22. K.A, P. (2017). *Indian Penal Code* (4 ed.). Lucknow: Eastern Book Company.
23. K.D, G. (2016). *A Text Book On Indian Penal Code* (6 ed.). Delhi: Universal Law Publishing.
24. Muthukumaran, D. B. (2008, January). Cyber Crime Scenario in India. *Criminal Investigation Department Review.*
25. Singh, P. D., & Loura, D. (2021). Cyber Security in Civil Aviation: Current Trends. *Dehradun Law Review, 13*(1), 95-105.
26. Vakul Sharma, I. T. (2011). In S. Vakul, *Information Technology Law and Practice* . New Delhi: Universal law publishing.