IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11440

Identification and Mitigation of Cyber Crimes against Women in India

Deepak Kumar Verma[1], Vinodini Verma[2], Anamika Pal[3], Drishti Verma[4]

[1]Assistant Professor, Department of Computer Science,
Dr. Rammanohar Lohia Avadh University, Ayodhya, India

[2]Assistant Professor, Department of Adult and Continuing Education,
Dr. Rammanohar Lohia Avadh University, Ayodhya, India

[3,4]Student, Department of Computer Science,
Dr. Rammanohar Lohia Avadh University, Ayodhya, India

Abstract: The internet has produced a difficult issue for females relating to cyber security in the present era of digitization. Girls and women are constantly confronted with issues such as privacy invasion-emails, e-chats, hate speech, online grooming, spoofing, sexual misbehavior, bullying, hacking, cyber stalking, transmitting morphing, obscene materials and sexual defamation, blackmailing misrepresentation and financial gain or espionage. Low computer literacy and internet illiteracy among women is also a major source of victimization. Online abuse, rather than being a means of communication, is literally famous as a type of abuse or violence against women and girls. Privacy infringement, illegal monitoring, cyber stalking, unlawful access to data, and retaliation are all becoming increasingly sophisticated in the IT business.

Key Words: Cyber crime, cyber security, cyber space, cyber law.

I. INTRODUCTION

Cybercrime is defined as illicit behaviour aiming at the security of computer systems and the data they process through electronic activities. In a broader sense, cybercrime refers to any criminal activity carried out using or in relation to a computer system or network, including illegal possession and the offering or distribution of information via a computer system or network. [1] Computer-crime is made up of two parts: the computer and the crime.

According to a statista [2] study, India had a considerable increase in cyber-crime recorded in 2020 compared to the previous year, as indicated in table 1. Over 50 thousand cyber-crime instances were reported that year. During the time period studied, Karnataka and Uttar Pradesh had the largest proportion.

In comparison to the rest of the country, the northern state of Uttar Pradesh had the largest number of cyber crimes, with over 6,000 incidents reported to authorities in 2018. Karnataka, India's IT state, followed suit the next year. The bulk of these complaints were filed under the Information Technology Act with the intent of defrauding or sexually exploiting victims.

Table -1: cyber-crimes reported in India (2012-2020)

Year	Number of cyber-crimes reported across India
2012	3,477
2013	5,693
2014	9,622
2015	11,592
2016	12,317
2017	21,796
2018	27,248

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11440

2019	44,546
2020	50,035

Source: https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

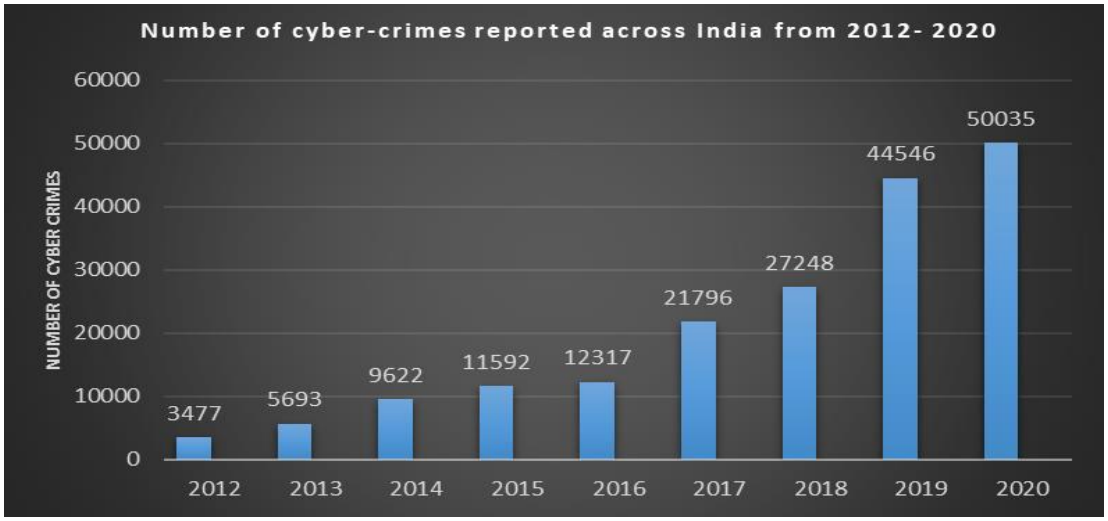


Chart-1: cyber-crimes reported across India (2012-2020)

According to a report of National Crime Records Bureau (NCRB) for the year 2020 number of cyber crimes reported in different states of India are tabulated in table 2. The table shows the data of cyber crimes in all states and union territories of india separately for the reported cases in the year 2020. The highest cases are reported in Karnataka and Maharashtra state.

Table -2: State wise cyber-crimes reported in 2020.

STATES/UT	TOTAL CYBER CRIMES
Andhra Pradesh	375
Arunachal Pradesh	1
Assam	1071
Bihar	47
Chhattisgarh	117
Goa	19
Gujarat	277
Haryana	222
Himachal Pradesh	52
Jharkhand	20
Karnataka	2859
Kerala	246
Madhya Pradesh	274
Maharashtra	1632
Manipur	26
Meghalaya	39
Mizoram	1
Nagaland	2
Odisha	560
Punjab	110
Rajasthan	238
Sikkim	0
Tamil Nadu	306

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11440

Telangana	649
Tripura	3
Uttar Pradesh	749
Uttarakhand	72
West Bengal	344
A&N Islands	3
Chandigarh	10
D&N Haveli andDaman & Diu	3
Delhi	51
Jammu & Kashmir	25
Ladakh	0
Lakshadweep	2
Puducherry	0

II. LITERATURE SURVEY

Ritu Kohli case was first cyber-sex crime which was reported in India. In this case one Manish Kathuria was arrested by officials of crime branch of Delhi Police for stalking an Indian lady Ms. Ritu Kohli by illegally chatting on website "MIRC" using her name. He used obscene and obnoxious language and distributed her residence telephone numbers, inviting people to chat with her on phone. As a result of this, Ritu kept getting obscene calls from everywhere. In a state of shock, she called the Delhi police and reported the matter. The police promptly swung into action, traced the culprit and started criminal proceedings against him under sec 67 of IT Act read with sec 509 of IPC for outraging Ritu Kohli's modesty.[3]

The first ever conviction in India for cyber pornography, was in the case of Suhas Katti v. State of Tamil Nadu in 2004, The court held that Katti Punished with two years rigorous imprisonment and fine 500/- under section 469 IPC, one year's simple imprisonment under section 509 of IPC and two years rigorous imprisonment and rupees four thousand fine for the offence Under Section 67 of IT ACT 2000 (Punishment for publishing or transmitting obscene material in electronic form).[4]

The recent Air Force Balbharati School case (Delhi) 2013 comes under this category where a student of the School was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at his tormentors and scanned photograph of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. The father of one of the class girls featured on the website came to know about this and lodged a complaint with the police. Such acts can be penalized under I.T. Act, 2000 and attracts sec. 43 & 66 of the said Act. The violator can also be booked under IPC sec 509 also.[5]

The very first instance of cyber defamation in India was recorded in the case of SMC Pneumatics (India) Pvt. Ltd. v. JogeshKwatra-Jogesh Kwatra [6] cyber defamation was reported when a company's employee (defendant) started sending derogatory, defamatory and obscene e-mails about its Managing Director. The e-mails were anonymous and frequent, and were sent to many of their business associates to tarnish the image and goodwill of the plaintiff company. The plaintiff was able to identify the defendant with the help of a private computer expert and moved the Delhi High Court. The court granted an ad-interim injunction and restrained the employee from sending, publishing and transmitting e-mails, which are defamatory or derogatory to the plaintiffs.

The most popular case of cyber spoofing is Gujarat Ambuja's Executive Case (1998) AIR 2000 MP 194, 2000 (2) MPHT 112 where the perpetrator pretended to be a girl for cheating and blackmailing the Abu Dhabi based NRI.

The first conviction in a cyber-stalking case against a woman in Maharashtra took place in July 2015 in the case of Yogesh Prabhu v. State of Maharashtra, decided by the additional chief metropolitan magistrate M.R. Natu, the magistrate convicted Prabhu under section 509 IPC and section 66E of the Information Technology Act 2008 (Punishment for violation of privacy).[7]

In a case of defamation, the Delhi High Court in Imtiaz Ahmed v. Durdana Zamir (2009 SCC online Del 477: (2009) 109 DRJ 357: 2009 INDLAW Del 119.) held the test of defamatory nature of a statement is its tendency to incite an adverse opinion or feeling of other persons towards the plaintiff. A statement is to be judged by the standard of the ordinary, right thinking members of the society at the relevant time. The words must have resulted in the plaintiff to be shunned or evaded or regarded with the feeling of hatred, contempt, ridicule, fear, dislike or disrespect or to convey an imputation to him or disparaging him or his office, profession, calling, trade or business. The plaintiff in such a case has

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022
DOI: 10.17148/IJARCCE.2022.11440

a right to be compensated in monetary term by the defendant. When one person sullies the good name of another out of inadvertence or the tort of defamation making the quinces, then it will amount to the tort of defamation making the defendant liable to pay damages as fixed by the court. The law related to the tort in India is still unmodified.[8]

The DPS MMS scandal [9] is a very famous case of this where an MMS clip of a school girl in compromising situation was made and distributed amongst various internet networks. In another incident, at Mumbai, a Swiss couple gathered slum children and then forced them to appear for obscene photographs, which they took and then uploaded those photographs to websites specially designed for paedophiles. The Mumbai police arrested the couples for pornography[10]. The most recent example is of Delhi Metro CCTV footage leaks case[11], where the CCTV recording couples getting intimate in metro stations etc. which has been recorded by police security cameras has been leaked on internet.

III. REASONS BEHIND VICTIMIZATION OF FEMALES

Gender Identities

Women sustain harm to their identities as a female. Women may feel impelled to compromise their female identity by "passing" as men to prevent discrimination. Female bloggers and commentators assume gender-disguising names to prevent cyber harassment. Even individuals who present themselves as women may nonetheless feel forced to "cover," i.e., engage in stereotypically male conduct, to avoid online abuse. Women play down stereotypically female attributes, such as compassion, and high- light stereotypically male ones, such as aggressiveness, to deflect cyber assaults. Cyber gender harassment undermines women's ability to achieve their professional goals. It may impair women's work directly such as technological attacks designed to shutter feminist websites and to discourage employees from hiring women. It may take a more indirect form of professional sabotage by discrediting women's competence in their careers.[12]

Fear of Defamation in Society

Most of the cybercrimes with women as victims remain unreported due to the hesitancy and shyness, her fear of defamation of family's name. Many times she considers that she herself is accountable for the crime done to her. The women are more helpless to the threat of cybercrime as the perpetrator's identity remains anonymous and he may constantly threaten and blackmail the victim with different names and identities. Due to these fears women often fail to report the crimes, causing the spirits of culprits to get even higher.[13]

Lack of Proper Universal and Domestic Laws to Address the Problem of Cyber-Attacks on Women

The information communication and technology (ICT) act was passed in 2006 and amended in 2013 with the aim of implementing the National and Communication Technology Policy 2002. The policy was taken in 2002 to draw attention for legislation to protect against cybercrimes and to ensure the security of data and freedom of information. Though the Act was enacted to protect the cyber victims but it doesn't cover the whole things of cybercrimes. Nowadays, women are frequently harassed over the internet or through mobile phones. Regrettably, there is no comprehensive law adequately dealing with sexual harassment in social media and other digital platforms, albeit cases can be filed under the Women and Children Repression Prevention Act, 2000, the Information and Communications Technology (ICT) Act, 2006, and the Pornography Control Act, 2012 or any other ordinary laws but the main problems is lack of sufficient machinery and lack of implementation the laws and legislature.[14]

Growing Popularity of the Multipurpose Social Networking Site (MPSNSs) for Forming Relationships

Facebook, Twitter, and Google-hosted social networking sites Google+ and YouTube have become imperative to our lives reason due to the craze and popularity of users. As has been stated above, MPSNSs provide a wide range of platforms for multitasking. The majority of users avail Facebook for forming relationships of various natures. The relationships thus formed may not abide by the settled rules and regulations restricting the human mind. Sharing real-life tragedies (how trivial they may be) through status messages may immediately attract a pool of supporters in the MPSNS, and these supporters and friends may also motivate the user to take action that they feel is absolutely right.[15]

Lack of Awareness by Female Users

One of the major reasons for the growth of sexual crimes in the Multipurpose Social Networking Sites (MPSNSs) is the lack of awareness of female users, who are the potential victims. As has been stated above, the majority of sexual crimes may happen when the victim herself allows the perpetrator to either access her private information or communicate with her. Many victims refuse to stop communication with the perpetrator or delete the profile information when attacked. Further, once victimized, many women victims and parents of minor victims immediately sought to contact the hackers to remove the offending posts or write back to the offender threatening him with terrible consequences. This irrational coping mechanism only leads to further victimization, as this helps the perpetrator to escalate the harassment.[16]

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11440

Benevolent Behaviour of Women

In this way, the user may either become the victim of groomers if the user is a woman, generate sympathy by sharing details about the ex-partner, colleague, and so on, who may be further targeted by such supporters. Similarly, in the case of online relationships, trivial disagreements can be published, and if the disagreement arises against a woman it leaves her literally stripped in public. In this way, when the fake avatars are created, the user may get another group of supporters who may start liking the fake avatar for the sexual contents and thus increase the embarrassment of the victim. Facebook itself has confessed that many of the user profiles are fake. This boosts the perpetrator to continue with the wrongdoing.[17]

Patriarchal Society and Prejudice

The prevalence of patriarchy and prejudice is regarded as the most imperative in leading to the subordinate status of women. This system has been prevalent within the Indian society, since medieval times. The status of women was recognized to be merely in the implementation of household responsibilities, child development, paying attention to health care and in taking care of the needs and requirements of the elderly family members. They were not allowed to express their perspectives and viewpoints in the making of decisions or render an active participation in any religious, cultural, social, or political activities. They were required to follow the norms and instructions that have been put into operation by the male members. Patriarchal societies in most parts of the country give preference to the male children and discriminate against the girl children. Due to patriarchy and prejudice, girls and women are deprived of nutrition, health care, education and employment. They have no more options to learn modern education, skill and technology.[18]

Unsupportable Behaviour of Police and Administration

The police usually uses the following grounds for refusing to take a complaint:

i. There is no specific proof to show that the harasser has been actually indicating the particular victim, even if he had used her name in the defamatory write-ups.

ii. The harasser has been practicing his right to speech. The police cannot curtail anyone's right to speech without solid evidence.[19]

Moreover some another reasons to easily victimizations of women can be no minimum age to join cyber communities like Facebook, Orkut, Myspace, Instagram, allow others to use one's own emails id, profile id password etc., ignorance to use safety tips like filtering emails, locking personal albums and information, personal walls of social network sites, share personal information, emotions with virtual friends, chat room patterns etc. whom you don't know in real life, ignoring policy guidelines of social networking sites ISPs etc.

IV. PATTERNS IDENTIFICATION FOR CYBER CRIMES

Creation of Fake Avatar of Women

Sexual offences against women on Multipurpose Social Networking Sites (MPSNSs) are most likely to occur when harassers create phoney avatars of the victims. Fake avatars can be defined as a false representation of the victim created by the perpetrator using digital technology, with or without the victim's visual images, and carrying verbal information about the victim that may or may not be entirely true, and which is created and circulated on the internet to intentionally harm the victim's character and mislead the viewers about the victim's original identity.

Sending Sexual Messages

While creating a phoney avatar is one of the most common ways to sexually victimise women, sending sexual messages to the victim is another sexual crime that may occur on Multipurpose Social Networking Sites (MPSNSs). This can be accomplished in one of three ways: (a) grooming women for sexual crime, (b) conversing on MPSNSs, or (c) bullying. The comments may be directed at the victim and posted in open forums so that other members of the group may see the sexually abusive postings.

Cyber-Aided Sexual Violence against Women

Friends and close friends can tag a user to any location, photo, or status post on social networking platforms like Facebook, Twitter, and others, allowing those who are not friends with the user to see the person's information. Similarly, if the user prefers to keep the profile private and limited exclusively to those followers, status updates and personal information can be limited to followers on Twitter. However, if a user decides to share her information with the rest of the world, neither Facebook nor Twitter prevents anybody from accessing and viewing the primary data. Given these circumstances, the user is vulnerable to physical assault as well as online harassment when using cyber assistance.

Cyber Stalking

This is one of the most well publicised cyber crimes in today's globe. Cyber stalking include tracking a person's online travels by leaving messages on bulletin boards frequented by the victim, accessing chat rooms frequented by the victim,

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11440

continually bombarding the victim with emails, and so on. Cyber stalking is more common among women who are pursued by men. Cyber stalkers use websites, chat rooms, discussion forums, open publishing websites, and email to track down and harass their victims. Stalkers may be motivated by four factors: sexual harassment, preoccupation with love, vengeance and hatred, ego and power trips.

Cyber Defamation

Another widespread crime against women on the internet is cyber tort, which includes libel and slander. This happens when defamation is carried out via computers and/or the Internet. In the matter of SMC Pneumatics (India) Pvt. Ltd. v. SMC Pneumatics (India) Pvt. Ltd. v. SMC Pneumatics (India) Pvt. Ltd. v. SMC Pneumatics (India) Pvt. Ltd. v. SMC P Jogesh Kwatra, Jogesh Kwatra, Jogesh Kwatra, Jogesh Kwatra, Jogesh Kwatra, Jogesh Kwatra When a company's employee (defendant) began sending disparaging, defamatory, and obscene e-mails about its Managing Director, it was reported as cyber defamation. The e-mails were anonymous and frequent, and they were sent to many of their business colleagues in order to smear the plaintiff company's reputation and goodwill. With the aid of a private computer expert, the plaintiff was able to identify the defendant and filed a case in the Delhi High Court. An ad-interim injunction was obtained by the court.

Morphing

Morphing is editing the original picture so as to make it look completely or largely different. Often criminally minded elements of the cyber world download pictures of girls from websites such as Facebook and then morph it with another picture in compromising situation so as to represent that those women were indulging in such acts. Often the next step after this is to blackmail those women through the threat of releasing the morphed images and diminishing the status of those women in society.

Email Spoofing

E-mail spoofing is a term used to describe fraudulent email activity in which the sender's address and other parts of the email header are altered to appear as though the email originated from a different source; it is done by properties of the email, such as the From, Return-Path and Reply-To fields, ill-intentioned users can make the email appear to be from someone other than the actual sender. This method is often used by cyber criminals to extract personal information and private images from unsuspecting women, these images are then used to blackmail those women.

Cyber Blackmailing

In this type of cyber-crime the sender demands something to recipient, otherwise sender promises to reveal her private information/ portray her in false manner/ do harm to her reputation etc.

Cyber Hate Propaganda

Means offensive communication between sender and multiple recipients with intend to spread hatred against a particular individual for her opinion, race, gender etc. One more cyber-crime against the women like cyber grooming, cyber bullying, forced pornography, obscenity and offensive communication etc.

Table 3: Patterns of cyber-crimes reported in 2020.

Type / Pattern of Cyber-crime against women in India in 2020	Total cases
Cyber blackmailing /threatening	74
Cyber pornography /hosting/publishing obscene sexual materials	1655
Cyber stalking/cyber bullying of women	887
Defamation /morphing of women	251
Fake profile	354
Other crimes against women	7184

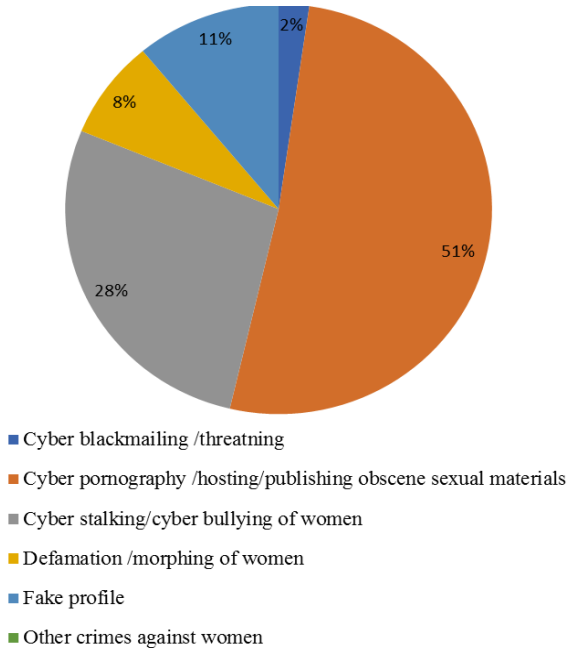


Chart-2: Patterns of cyber-crimes reported across India.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

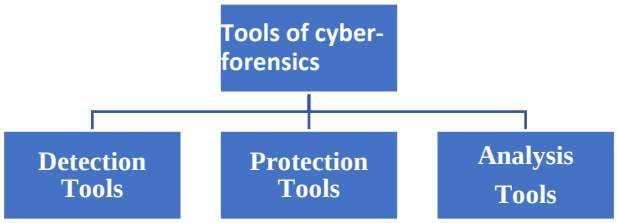
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11440

V. TOOLS FOR MITIGATION AND GUIDELINES FOR REMEDIAL MEASURES TO PREVENT CYBER-CRIMES

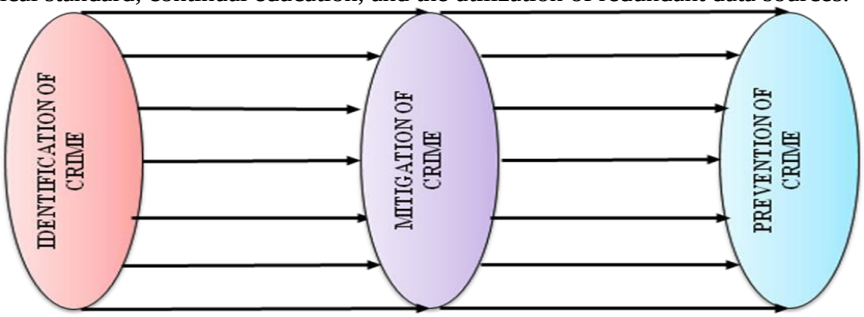
Cyber-forensics tools are classified into three categories: detection tools, protection tools, and analysis tools.



Risks are identified using detection techniques. They begin with network-based tools, such as Nmap, which is one of the most extensively used. Operating system identification using TCP/IP fingerprinting is one of the tool's distinctive characteristics. Another tool is Nessus, a host-based scanner that looks for particular vulnerabilities on a certain host. It's a vulnerability scanner with a great user interface. Another great scanner is Retina. In real-world investigative settings, more than one tool is employed. To test a web server for vulnerabilities, for example, one would run Nmap, then Nessus, and finally a scan.

The risk that the detection tools indicate is mitigated by protection technologies. They reduce the risk by raising the number of network or host-based countermeasures in the risk calculation. Routers, which direct traffic to the appropriate destination, are usually the first line of defence for a network. Firewalls are the second line of protection in a secure network, and they reduce risk by acting as a sentry for the network, allowing only traffic that has been properly authorised to get through. Intrusion detection systems (IDSs) act as network burglar alarms by detecting malicious traffic using signatures. IDS systems like Snort are an excellent example. They reduce danger by raising awareness and understanding.

Risk is assessed using analytical methods. They assess what happened, how it happened, and what the repercussions were. The Coroners toolkit, which runs on NIX, and EnCase, which runs on Windows, are two examples of analytic tools. It is impossible to overstate the necessity of having a good technical skill to use these toolkits. Certain conditions must be satisfied while working with cyber-forensics. These qualities include technical awareness (knowledge of the technical consequences of actions), comprehension of how data may be manipulated, cunning, open-mindedness, deception, a high ethical standard, continual education, and the utilization of redundant data sources.



VI. CONCLUSION

Women do not have the same amount or forms of desirable privacy in cyberspace as males. Computer use, as well as the use of mobile devices to connect to the Internet and share data, are increasingly commonplace. The way consumers obtain information and build relationships has altered in cyberspace, and this has had a significant impact on our work, communications, and social interactions. Of course, when data and other things are moved into cyberspace, many types of cybercrime are also conveyed. Because the amount of personal information that individuals communicate and post on the Internet is fast expanding, particularly with the increasing popularity of social networks, new cybercrimes are developing, such as those related to social networks. Cyber-stalking, e-mail harassment, cyber bullying, morphing, email spoofing, and cyber defamation are all covered by laws and regulations. The extent to which the user is aware of the harm he or she has endured in cyberspace has real-world implications. This predicament arises from a lack of understanding in specific areas, which is exacerbated by the fact that information technology is now accessible to anybody. We will examine fear of cybercrime in different sectors in future study and try to figure out how people' perceptions of cyber risks, and hence their fear of cybercrime, may be reduced through education.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11440

REFERENCES

[1] H.V. Milner,the political economy of international trade ,Annual review of political science,2 (1999)

[2] https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

[3] http://cyberlaws.net/cyberindia/2CYBER27.htm

[4] http://www.naavi.org/cl_editorial_04/suhas_katti_case.htm.

[5] Abhimanyu Behera, " Cyber Crimes and Law In India," XXXI,IJCC 19 (2010)

[6] http://cyberlaws.net/cyberindia/defamation.htm

[7] Prasanto k Roy, Why Online Harassment Goes Unpunished in India, (15 March 2015), http://www.bbc.com/ews/world-asia-india-33532706

[8] Talat Fatima, Cyber Crimes 147-148, (Eastern Book company, Lucknow, 2016)

[9] http://en.wikipedia.org/wiki/DPS_MMS_Scandal

[10] G. Rathinasabapathy and L. Rajendran, " Cyber Crimes and Information Frauds: Emerging Challenges For LIS Professionals," Conference on Recent Advances in Science & Technology (2007)

[11] http://zeenews.india.com/news/nation/porn-mmses-from-delhi-metro-cctv-footage_860933.html

[12] Danielle Keats Citron, Law's Expressive Value in Combating Cyber Gender Harassment, 108(3) Michigan Law Review, 373-415 (Dec., 2009).

[13] Yogesh Bama, Criminal Activities in Cyber-word 36, (Dominent Pubhshers and Distributers, New Delhi, 2005)

[14] R.K. Choubey, An Introduction to cyber-crime & cyber law. 123, (ed-2008, Kama! Law House, Kolkata, 2009)

[15] Debarati Halder and K. Jaishankar, Patterns of Sexual Victimization of Children and Women in the Multipurpose Social Networking Sites, (2014);

[16] Catherine D.Marcum and George E. Higgins, Social Networking as a Criminal Enterprises, CRC Press,138.

[17] S.V. Rao Joga, Law of Cyber Crimes & Information Technology Law 85, (Wadhwa, Nagpur India, 2004)

[18] TalatFatima, Cyber Crimes 58, (Eastern Book Company, Lucknow, 2011).

[19] Rajesh Kumar Goutam and Deepak Kumar Verma, Top Five Cyber Frauds, International Journal of Computer Applications 119(7):23-25, June 2015

[20] Inder S. Rana, Law of obscenity in India 96, (Mittal Publications, New Delhi, 1990).