iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VII **Month of publication:** July 2020

DOI: https://doi.org/10.22214/ijraset.2020.30295

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

Cyber Crime against Women in the Digital ERA: A Breif Indian Scenerio

Upasana Borah
Student, BBA LL.B(HONS), N.E.F Law College, Guwahati, Assam

Abstract: ***In India, online harassment of women and marginalized genders and sexualities is widespread, as opposed to Internet's underlying reason of equivalent chance and impartiality. What we have today is an imperfect web that mirrors the disconnected world we live in, where ladies and minimized networks are mishandled, badgering, compromised, followed and disregarded every day. This exploration paper plans to break down the novel dangers that ladies and underestimated segments in India face on the web and how Indian laws influence these issues. Laws, Rights and Regulations is a one of a kind and significant commitment to the writing on digital wrongdoing. It investigates gendered measurements of digital violations like grown-up tormenting, digital following, hacking, maligning, transformed obscene pictures, and electronic extorting. These and different strategies intended to deliver terrorizing, control, and different damages are much of the time submitted by culprits who, for some, reasons, are probably not going to be recognized or rebuffed. Researchers, scientists, administrators, and common ladies and their supporters will increase a superior comprehension of digital exploitation and find how to improve reactions to digital crimes against women.. Cyber crime has caused a lot of harm to the individual group of people, associations, and even the Government. Cybercrime identification strategies and order techniques have concocted fluctuating degrees of accomplishment for forestalling and shielding information from such assaults. A few laws and techniques/methods have been acquainted all together with forestall cybercrime and the punishments are set down to the criminals.***

Keywords: Digital Exploitation, Information Technology, Hacking, Electronic extorting

I. RESEARCH METHODOLOGY

The paper utilizes both subjective and quantitative exploration, including examination of media reports including on the web provocation of prominent ladies; an overview of 500 web-based social networking clients; and meetings with ten of the respondents. This paper is primarily based paper where we tend to treat the methodology of cyber crime which gives an better insight of the topic and scope for research. The secondary data is been collected from websites, international journal and articles.

II. INTRODUCTION

Information Technology solutions have paved a manner to a new global of internet, business networking and e-banking, budding as a solution to reduce costs, trade the sophisticated monetary affairs to greater easier, speedy, efficient, and time saving method of transactions. Internet has emerged as a blessing for the existing tempo of life however at the equal time also resulted in numerous threats to the purchasers and other establishments for which it's proved to be maximum beneficial. Various criminals like hackers, crackers have been capable of pave their manner to intervene with the internet accounts thru numerous strategies like hacking the Domain Name Server (DNS), Internet Provider's (IP) address, spoofing, phishing, net phishing etc. and feature been a success in gaining "unauthorised access" to the user's laptop system and stolen useful facts to gain huge profits from customer's accounts. Intentional use of Information Technology by way of cyber terrorists for generating negative and harmful effects to tangible and intangible property of others is called "Cyber Crime".

[i] Cyber crime is definitely an international problem with no countrywide boundaries. Hacking assaults can be released from any nook of the world with none worry of being traced or prosecuted easily. Cyber terrorists normally use the pc as a tool, target, or both for their unlawful act either to gain information which can bring about heavy loss/ harm to the owner of that intangible sensitive facts. Internet is one of the means by way of which the offenders can benefit such price sensitive statistics of companies, companies, individuals, banks, intellectual property crimes (along with stealing new product plans, its description, marketplace programme plans, the listing of clients etc.), selling illegal articles, pornography etc. This is done thru many methods which include phishing, spoofing, pharming, internet phishing, twine transfer etc. And use it to their own benefit without the consent of the individual. Many banks, economic institutions, funding houses, brokering corporations etc. Are being victimized and threatened by way of the cyber terrorists to pay extortion cash to preserve their sensitive information intact to avoid massive damages. And it's been pronounced that many establishments in US, Britain and Europe have secretly paid them to prevent massive meltdown or collapse of self belief

amongst their customers. In India, the Information Technology Act 2000 changed into enacted after the United Nation General Assembly Resolution A/RES/51/162, dated the 30th January, 1997 through adopting the Model Law on Electronic Commerce adopted with the aid of the United Nations Commission on International Trade Law. This was the primary step toward the Law regarding e-trade at international stage to regulate an alternative shape of commerce and to offer prison status in the area of e- trade. It becomes enacted thinking of UNICITRAL version of Law on e- trade 1996.

Some Noteworthy Provisions Under The Information Technology Act, 2000:-

Sec.43 Damage to Computer system etc.	Compensation for Rupees 1crore.
Sec.66 Hacking (with intent or knowledge)	Fine of 2 lakh rupees, and imprisonment for 3 years.
Sec.67 Publication of obscene material in e-form	Fine of 1 lakh rupees, and imprisonment of 5years, and double conviction on second offence.
Sec.68 Not complying with directions of Controller.	Fine upto 2 lakh and imprisonment of 3 years.
Sec.70 Attempting or securing access to computer.	Imprisonment upto 10 years.
Sec.72 For breaking confidentiality of the information of computer	Fine upto 1 lakh and imprisonment upto 2 years.
Sec.73 Publishing false digital signatures, false in certain particulars.	Fine of 1 lakh, or imprisonment of 2 years or both.

III. NEGATIVE USE OF INFORMATION TECHNOLOGY BY HACKERS

Hacker is laptop expert who uses his information to benefit unauthorized get admission to the pc network. He's now not any person who intends to break thru the device but also includes person who has no purpose to harm the machine but intends to learn extra by using one's laptop. Information Technology Act 2000 doesn't make hacking in keeping with se an offence however appears into component of mens rea.

Crackers on other hand use the information reason disruption to the community for non-public and political motives. Hacking via an insider or an employee is quite outstanding in gift date. Section 66 (b) of the Information Technology Act 2000, provides punishment of imprisonment for the term of 3 years and first-rate which may extent to two lakhs rupees, or with both.

1) *Computer Viruses:* Viruses are utilized by Hackers to contaminate the user's pc and damage information saved on the pc through use of "payload" in viruses which contains unfavourable code. Person would be liable under I.T Act handiest whilst the consent of the owner isn't always taken before inserting virus in his device. The contradiction here is that though certain viruses reasons temporary interruption by means of showing messages on the screen of the user however nevertheless it's now not punishable beneath Information Technology Act 2000 because it doesn't purpose tangible harm. But, it must be made punishable as it would fall below the ambit of 'unauthorised get entry to' though doesn't motive any damage.
2) *Phishing:* By the use of email messages which absolutely resembles the authentic mail messages of customers, hackers can ask for verification of certain statistics, like account numbers or passwords etc. here customer may not have knowledge that the e-mail messages are deceiving and would fail to perceive the originality of the messages, this outcomes in massive financial loss when the hackers use that records for fraudulent acts like withdrawing cash from clients account without him having expertise of it.
3) *Spoofing:* This is carried on by way of use of deceiving Websites or e-mails. These resources mimic the original web sites so nicely with the aid of use of logos, names, graphics or even the code of actual bank's site.
4) *Phone Phishing:* Is achieved by means of use of in-voice messages by way of the hackers wherein the customers are asked to reveal their account identification, and passwords to report a complaint for any problems regarding their money owed with banks etc.
5) [ii] *Internet Pharming:* Hacker right here objectives at redirecting the website utilized by the purchaser to another bogus website via hijacking the victim's DNS server (they are computers responsible for resolving internet names into actual addresses - "signposts of internet), and converting his I.P cope with to fake internet site by way of manipulating DNS server. This redirects user's authentic internet site to a false misleading website to advantage unauthorised statistics.

6) *Risk Posed On Banks And Other Institutions:* Wire transfer is the manner of transferring cash from one account another or transferring cash at cash office. This is maximum convenient manner of transfer of cash by customers and money laundering by means of cyber terrorists. There are many tips issued by means of Reserve Bank of India (RBI) on this regard, considered one of which is KYC (Know Your Customer) norms of 2002.

Main goal of that is to:

a) Ensure suitable consumer identification, and

b) Monitor the transaction of suspicious nature and file it to suitable authority each day bases.

7) *Publishing Pornographic Material In Electronic Form:* Section sixty seven of the Information Technology Act, 2000 in parallel to Section 292 of Indian Penal Code, 1860 makes booklet and transmission of any fabric in electronic that's lascivious or appeals to the prurient hobby a crime, and punishable with imprisonment which may extend to five years and quality of 1 lakh rupees and subsequent offence with an imprisonment extending to 10 years and quality of two lakhs. Various tests had been laid down regularly in direction of time to determine the real crime in case of obscene cloth published in electronic form on net. There's very thin line existing among a material which can be referred to as obscene and the one that is artistic. Court even pressured on want to keep balance among fundamental proper of freedom of speech and expression and public decency and morality. If rely is in all likelihood to corrupt and corrupt those minds which are open to influence to whim the material is in all likelihood to fall. Where both obscenity and inventive count is so blended up that obscenity falls into shadow as its insignificant then obscenity can be overlooked.

8) *Investment Newsletter:* We commonly get newsletter presenting us free information recommending that funding in which area would be profitable. These may now and again be a fraud and may motive us massive loss if relied upon. False information can be spread by way of this technique approximately any organization and can purpose massive inconvenience or loss via junk mails online.

9) *Credit Card Fraud:* Huge loss may motive to the victim because of this form of fraud. This is finished with the aid of publishing false virtual signatures. Most of the humans lose credit cards on the way of delivery to the recipient or its damaged or defective, misrepresented etc.

IV. AN OVERVIEW TO DATA PROTECTION LAWS

Data protection is the most common process of safeguarding important information from getting it corrupt .The most important principle of Data Protection is to protect and safeguard the data and make it available under the circumstances . It is always be applied to all forms of data either personal or corporate which deals with both integrity and protection of data. Protecting the privacy of the people in the modern era is essential to an good effective democratic government. However, increasing number of awareness and recognition for data protection across the world is still lack of legal infrastructure to protect the RIGHT TO PRIVACY which is regarded as FUNDAMENTAL RIGHT under ARTICLE 21 of the INDIAN CONSTITUTION.

V. HISTORY OF DATA PROTECTION

In today's Digital World of ecosystem everyone has a valid e-mail address. Many people has e-mail accounts on free web-based e-mail platforms. Similarly Facebook account has a manifestation of our thoughts in a form of post . Technology has raced rapidly since past decades . Hence it is an old concept. Civilization ever since seems to be growing their advent and awareness were concerned about protection and preservation of their data. That is the reason why different civilizations had adopted different ways to protect data of every individual. Data has been sought to be protected from the beginning of human civilization. Over the period of time different kings and kingdoms tried to protect data by enshrining them in various forms of tangible mediums including stone. In fact, the focus of data protection is protecting the rights of individuals with respect of their data. The initiation of internet and the global explosion of growth in data have necessitated different nations to come up with their own distinct national legislation to deal with data protection. Not only this, even international organizations have been working on various principles pertaining to data protection.

VI. CONCEPT OF DATA PROTECTION

Internet is one of the most significant innovation in the human history after the advent of fire. No single event has impacted the growth of humanity so much as the internet. While the advent of internet has on the one hand made geography history and on the other hand ushered in the new data economy. The concept of data protection has emerged across the world. India has not endorsed any particular international approach in the context of data protection. Data protection has not been a priority as far as national legislation is concerned with. India distinctly lacks a dedicated legislation on data protection. However many countries like United Kingdom , European Union has passed influential legislation on pertaining to data protection.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

VII. DEFINITION OF DATA PROTECTION

Data Protection has been defined in different manner and styles by different sources and legal entities. According to Collinsdictionary.com , data protection means, ”safeguards for individuals relating to personal data stored on computer”.
Dataprotection.eu has defined the term data protection as, “a type of privacy protection manifesting in special legal regulation. Data Protection right ensures a person the right of disposal over all data in connection with his personality”.
In simple words, data protection can also be defined as protection or safeguard of data from getting hacked or destroyed.
Data becomes extremely significant in our lives. It cannot be denied that we are continuously producing more and more electronic data on ourselves whether it is the output from our computer system.
Further Wikipedia defines Information Privacy/Data Protection as, “the relationship between the collection and dissemination of data, technology, the public expectation of privacy and also the legal and political issues surrounding them”.

VIII. DATA PROTECTION LAW IN INDIA

India has a dedicated mother legislation dealing with data and information in an electronic form i.e INFORMATION TECHNOLOGY ACT(I.T), 2000 . In India Cyber Law being the Information Technology Act, 2000 has various provisions which have an direct impact upon the protection and preservation of data and information. Initially the I.T Act was enacted to with the aim to facilitate electronic commerce or e-commerce but as time passed by technologies rapidly got changed with new innovation and replaced by other technologies which compelled the lawmakers to amend the I.T ACT, 2000.

IX. LIABILITY FOR BREACH OF E-DATA CIVIL OR CRIMINAL

SEC 43 of the INFORMATION TECHNOLOGY, 2000 is an extremely important provision under the I.T ACT, 2000 as it deals with penalty and compensation for damage to computer , computer system, data or computer database information resident in such computer or computer system. The law of tort in the country is not well developed even after more than 60 years of independence and not much progress has been made in this discipline of law. One of the primary objects of any data protection legal regime is to ensure that electronic data should not be able to accessed or used in an unauthorised manner.

X. INDIAN PENAL CODE

The Indian Penal code doesn't specifically address breaches of knowledge privacy. Under the Indian Penal code, liability for such breaches must be inferred from related crimes. [iii] Section 403 of the IPC,1860 imposes criminal penalty for dishonest misappropriation or conversion of “movable property” for one’s own use.

XI. CYBER CRIME IN DIGITAL ERA AGAINST WOMEN

Cybercrime went up by 6.3 %in 2016 (12,317) more than 2015 (11,592). Uttar Pradesh (2,639 cases, 21.4%) announced the most cases, trailed by Maharashtra with 19.3 %(2,380 cases) and Karnataka with 8.9 % (1,101 cases). A few cybercrimes of 2016 are given in National Crime Records Bureau (NCRB) of India doesn't keep up any different record of digital wrongdoings against kids and Women.

XII. CRIME AGAINST WOMAN

"Digital wrongdoings against women and kids are on the raise and they have been definitely deceived in the internet" Some culprits attempt to stigmatize women and youngsters by sending indecent messages, following women and kids by utilizing visit rooms, sites and so on., creating obscene recordings for the most part made without their assent, mocking messages, transforming of pictures for obscene substance and so on.
Indian women can't report cybercrimes right away. The greater part of the issues can be comprehended if ladies report the wrongdoing promptly and cautions the victimizer about making more grounded move.
Cybercrimes are multiplying at a higher rate in India. For the most part, Virtual companions gain the certainty of their female companions and abuse the data of their female companions to intellectually annoy them. Such wrongdoings are significantly occurring in India and furthermore over the globe.
For example, extorting, undermining, tormenting, or cheating through email is finished by preparators.

XIII. SOCIOLOGICAL REASONS FOR THE GROWTH OF CYBER CRIME

The vast majority of the cybercrimes stay unreported because of the reluctance and modesty of the person in question what's more, her dread of slander of family's name. Commonly she thinks about that she herself is responsible for the wrongdoing done to her. The Women's are progressively defenseless against the peril of cybercrime as the perpetrator's personality stays unknown and he may continually undermine what's more, coercion the casualty with various names and personalities. Women dread that revealing the wrongdoing may make their family life hard for them, they additionally question whether they will get the help of their loved ones and what the impression of society will be on thinking about them. Because of these feelings of trepidation ladies regularly neglect to report the wrongdoings, causing the spirits of offenders to get much higher.

XIV. MEASURES AND PROPOSED SOLUTION FRAMEWORK

To Ample opportunity has already past to call for modernization of the preventive set up for cybercrimes and to prepared police faculty with reasonable information and aptitudes. A portion of the arrangement are given beneath:

1) NCRB ought to collect all the instances of lady and kid provocation and different cybercrimes against lady and kids under a different classification with the goal that exhibition of law implementation offices in such manner could be recognized and watched appropriately.
2) Law implementation offices and police power should be sharpened of the difficult features of digital wrongdoings against women and kids and their measurements to record and start activity against such wrongdoings should be reinforced critically.
3) There ought to be a Digital Police Portal or E-Portal where lady can report their issues on the web. This could decrease the quantity of cases under-announced due to related shame and penchant of guardians/gatekeepers to not include police in such issues the gateway likewise keeps up the database of crooks which could truly help law implementation.
4) It is expected to work together both police power and digital scientific laboratories together for better examination.

XV. DIGITAL CRIME MODEL PREVENTION MODEL PROPOSED FOR WOMEN.

This modelstands on three columns i.e., Education. Strengthening and lawful plan of action.

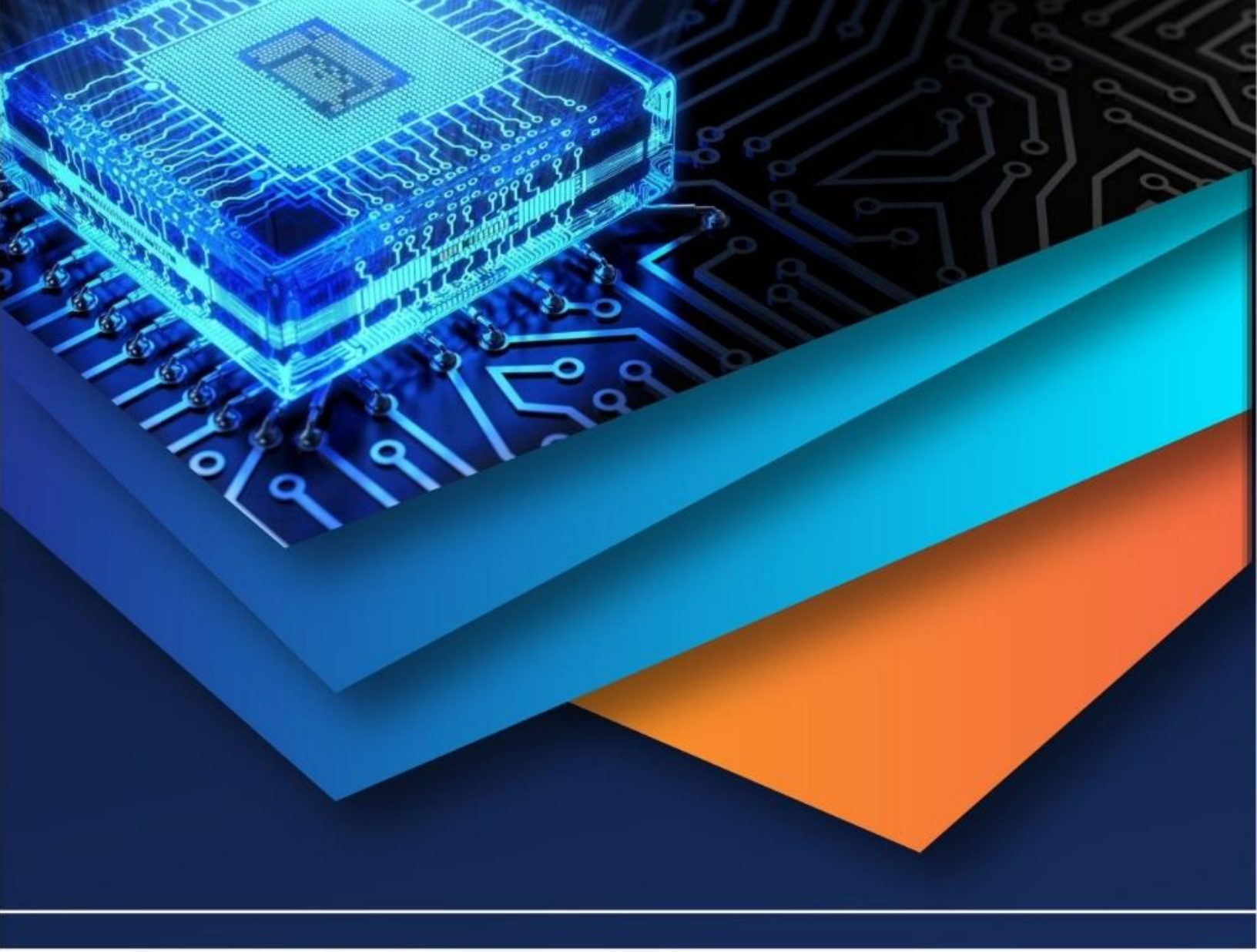
1) Education pillar reinforces the instruction system in terms of computerized India. Women often ought to get limit building classes or workshops from school level. These limit building workshops investigate information on handling cybercrimes by utilizing most recent advances young ladies ought to be made mindful about taking care of innovations and information with respect to security settings. It urges the lady to accomplish more investment in advanced media and be prepared to deal with issues in regards to cybercrimes. School educational program must cover all parts of cybercrimes and digital security. Along these lines, training framework must start contemporary issues relating to cybercrimes. School educational program ought to include following focuses as given beneath:
a) Digital world
b) Do‟s and Don‟t
c) Digital Etiquettes
d) E-Safety and security
e) Cyber Law to sum things up
f) Legal response
g) Prosecution
2) Empowerment pillar urges the lady to speak more loudly against cybercrime. This could make a domain where ladies have fairness on each level for example socially, financially, strategically, intellectually, etc.
a) Legal Empowerment should be possible by administering required standards and rules with their execution.
b) Social Empowerment: This could urge the casualties to speak loudly against their sufferings. NGOs can assume indispensable job to give a legitimate stage where casualties can get lawful and procedural direction.
c) Mental Empowerment: The most significant advance in the achievement of lady who battle against their badgering in advanced space. The best change can be brought by celebrating the victim's enthusiasm to battle out badgering.
3) Legitimate Recourse-This column will work like a scaffold and put an association between women what's more, law authorization. In this way, there ought to be a Digital police gateway for example e-entrance or e-courts where lady can report their issues on the web and venture towards cure at simple and safely with less time and exertion utilization. This could diminish the quantity of cases.

XVI. CONCLUSION

There is a requirement for consistent assessment of digital laws and method since ladies face challenges while looking for redressal because of the absence of mindfulness. In this paper, a few issues are being recognized and particular to these issues an anticipation model is proposed. This model could reinforce the lady and society. The police and the legislature, both have their parts to play, yet these digital violations will be downcasted when lawful advances are went with women attention to acquire a move the attitude of the general public on the loose. There should be proper implementation of laws regarding cyber crimes against women and kids.

REFERENCES

[1] https://legalserviceindia.com/article/l146-Cyber-Crime-And-Law.html
[2] https://educheer.com/essays/cyber-crimes-and-steps-to-prevent-and-control/
[3] https://www.jstor.org/stable/26441284



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY