International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1267-1275 www.ijaem.net ISSN: 2395-5252

Brief Study on Awareness about Cybercrime and Cyber laws In India

Mehakpreet kaur, Jaskirat Kaur
Department of Computer Science, Sri Guru Granth Sahib World University, Fatehgarh Sahib, India

Submitted: 05-05-2021 Revised: 18-05-2021 Accepted: 22-05-2021

ABSTRACT - As we all know that this is the era where most of the things are done usually over the internet starting from online dealing to the online transaction. Since the web is considered as worldwide stage, anyone can access the resources of the internet from anywhere. The internet technology has been using by the few people for criminal activities like unauthorized access to other's network, scams etc. Cybercrime involves computers and networks, any crime that is done using a computer or networking system is called cybercrime.Cybercrime increase day-day because the users are increasing. Cybercrime cover a wide range of various attacks such as Cyber theft, Cyberwarfare, growing Computer viruses or Malware, Internet scam, Spamming, Phishing, carding (cheating), child pornography and mental property claims crimes, etc. Because of increase in cyber-attacks these days, online users need to be aware of this variety of attacks and need attention while doing online transactions. It covers a broad area, encompassing many subtopics as well as freedom of expressions, access to and utilization of the Internet, and online security or online privacy. [Generically, it is eluded as the law of the web.] In this paper we will discuss about cybercrime and cyber law in India.

Keywords: Cybercrime, Malware, cyber law in India, child pornography, computer viruses, Internet, Unauthorized access, Cyberspace, Punish, Network.

I. INTRODUCTION: -

The invention of Computer has made the life of humans easier, it has been using for various purposes starting from the individual to large organizations across the globe. In simple term we can define computer as the machine that can stores and manipulate/process information or instruction that are instructed by the user. In a new study, it was reported that over 15 Indian towns, Mumbai, New Delhi, and Bengaluru have suffered the maximum amount of cyber-attacks .Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for other's benefit since decades. This gave birth to "Cyber Crime". This had led to the engagement in activities which are illegal tothe society. In the Annual Cyber Security Report by CISCO, 53% of cyber-attacks made more than $500K of economic loss to companies in 2018. India has faced a growth of 7.9% in data gaps since 2017[1]. Also, the normal cost per data crime record is rising to INR 4,552 ($64). Cyber-attacks against India have grown to such an area that our nation ranks fourth outside of the top 10 targeted nations in the world. In a statement by India Today, Chennai encountered the largest percentile of cyber-attacks among a stat of 48% in the opening portion of 2019. We can define Cyber Crime as the crimes committed using computers or computer network and are usually take place over the cyber space especially the Internet. No survey or warning has served any change in the cyber security management of organizations beyond the public. In contempt of seeing several cyber-attacks in India, people are still negative conscious of productive cyber-security answers to prevent their system from any other crime. Here are some modern series of cyber-attacks that massively realized loss to in famous companies in India.

Now comes the term "Cyber Law". Cyber Crimes, digital and electronic signatures, data protections and privacies etc are comprehended by the Cyber Law. The UN's General Assembly recommended the first IT Act of India which was based on the "United Nations Model Law on Electronic Commerce" (UNCITRAL)[2].

II. OBJECTIVE :-

The principle target of our paper is to spread the knowledge of the crimes or offences that take place through the internet or the cyberspace, along with the laws that are imposed against those crimes and criminals. We are additionally trying to focus on the safety in cyberspace.

III. CYBER CRIME AND CYBER LAW :-

Wecandefine"CyberCrime"asany malefactoror other offenceswhereelectronic communications or informationsystems,including anydeviceortheInternetorbothormoreofthem areinvolved[3].Wecandefine"Cyberlaw"asthe legal issues that are related toutilizeof communications technology, concretely "cyberspace",i.e.theInternet.Itisanendeavorto

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1267-1275 www.ijaem.net ISSN: 2395-5252

integrate the challenges presented by human action on the Internet with legacy system of laws applicable to the physical world. Cyber Law is the law governing cyber space. Cyber law encompasses laws relating to cybercrime, Electronic and Digital Signatures, Intellectual Property Data Protection and Privacy [4].

3.1 Cyber Crime:-Sussman and Heuston first proposed the term "Cyber Crime" in the year 1995. Cybercrime cannot be described as a single definition; it is best considered as a collection of acts or conducts. The cybercrime is also known as electronic crimes, computer-related crimes, e-crime, high technology crime, information age crime etc.

In simple term we can describe "Cyber Crime" are the offences or crimes that takes place over electronic communications or information systems. These types of crimes are basically the illegal activities in which a computer and a network are involved. The unusual characteristic of cybercrime is that the victim and the offender may never come into direct contact. Cybercriminals often opt to operate from countries with nonexistent or weak cybercrime laws in order to reduce the chances of detection and prosecution.

IV. HISTORY OF CYBER CRIME:-

The first Cyber Crime was recorded within the year 1820. The primeval type of computer has been in Japan, China and India since 3500 B.C, but Charles Babbage's analytical engine is considered as the time of present day computers. In the year 1820, in France a textile manufacturer named Joseph-Marie Jacquard created the loom. This device allowed a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard's workers that their livelihoods as well as their traditional employment were being threatened, and prefer to sabotage so as to discourage Jacquard so that the new technology cannot be utilized in the future.

V. CLASSIFICATIONS OF CYBER CRIME

Cyber Crime can be classified into four major categories. They are as follows:

a) Cyber Crime against individuals: Crimes that are committed by the cyber criminals against an individual or a person. A few cyber crimesagainst individuals are:

- Email spoofing: This technique is a forgery of an email header. This means that the message appears to have received from someone or somewhereother than the genuine or actual source [5]. These tactics are usually used in spam campaigns or in phishing, because people are probably going to open an electronic mail or an email when they think that the email has been sent by a legitimate source.

Phishing: In this type of crimes or fraud the attackers tries to gain information such as login information or account's information by masquerading as a reputable individual or entity in various communication channels or in email. Some other cyber crimes against individuals includes Net extortion, Hacking, Indecent exposure, Trafficking, Distribution, Posting, Credit Card, Malicious code etc. The potential harm of such a malefaction to an individual person can scarcely be bigger.

Cyber defamation: Cyber defamation means the harm that is brought on the reputation of an individual in the eyes of other individual through the cyber space. The purpose of making defamatory statement is to bring down the reputation of the individual.

b) Cyber Crime against property: These types of crimes includes vandalism of computers, Intellectual (Copyright, patented, trademark etc) Property Crimes Online threatening etc.

Intellectual property crime includes:

- Software privacy: It can be describes as the copying of software unauthorized.
- Copyright infringement: It can be described as the infringements of an individual or organization's copyright. In simple term it can also be describes as the using of copyright materials unauthorizedly such as music, software, text etc.
- Trademark infringement: It can be described as the using of a service mark or trademark unauthorizedly.

c. Cyber Crime against society: Cyber Crime against society includes:

- Forgery: Forgery means making of false document, signature, currency, revenue stamp etc.
- Web jacking: The term Web jacking has been derived from hi jacking. In this offence the attacker creates a fake website and when the victim opens the link a new page appears with the message and they need to click another link. If the victim clicks the link that looks real he will redirected to a fake page. These types of attacks are done to get entrance or to get access and controls the site of another. The attacker may also change the information of the victim's webpage.

d. Cyber Crime against organization: Cyber Crimes against organization are as follows:

- Unauthorized changing or deleting of data.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1267-1275 www.ijaem.net ISSN: 2395-5252

- Reading or copying of confidential information unauthorizedly, but the data are neither being change nor deleted.
- DOS attack: In this attack, the attacker floods the servers, systems or networks with traffic in order to overwhelm the victim resources and make it infeasible or difficult for the users to use them.
- Email bombing: It is a type of Net Abuse, where huge numbers of emails are sent to an email address in order to overflow or flood the mailbox with mails or to flood the server where the email address is.
- Salami attack:The other name of Salami attack is Salami slicing. In this attack, the attackers use an online database in order to seize the customer's information like bank details, credit card details etc. Attacker deduces very little amounts from every account over a period of time. In this attack, no complaint is file and the hackers remain free from detection as the clients remain unaware of the slicing. Some other cyber crimesagainst organization includes Logical bomb, Torjanhorse, Data diddling etc.

VI. CYBER CRIME'S SCENARIO IN INDIA(A FEW CASE STUDY)

1.Pune Citibank Mphasis Call Center Fraud :-

Some ex-employees of BPO arm of MPhasiS Ltd Sources defrauded US Customers of Citibank to the tune of Rs 1.5 crores. It was one of those cyber crime cases that raised concerns of many kinds including the role of "Data Protection"[6]. The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It istherefore firmly within the domain of "Cyber Crimes".ITA-2000 is versatile enough to accommodate the aspects of crime not covered by ITA-2000 but covered by other statutes since any IPC offence committed with the use of "Electronic Documents" can be considered as a crime with the use of a "Written Documents". "Cheating", "Conspiracy", "Breach of Trust", etc. are therefore applicable in the above case in addition to the section in ITA-2000.Under ITA-2000 the offence is recognized both under Section 66 and Section 43. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damages to the victims to the maximum extent of Rs 1 crore per victim for which the "Adjudication Process" can be invoked.

2. SMC Pneumatics (India) Pvt. Ltd. vs. JogeshKwatra

In India's first case of cyber defamation, the High Court of Delhi assumed jurisdiction over a matter where a corporation's reputation was being defamed through emails and passed an important ex-parteinjunction.Amongst the many cyber cases in India, in this case, the defendant JogeshKwatrabeing an employee of the plaintiff company started sending derogatory, defamatory, obscene, vulgar, filthy and abusive emails to his employers as also to different subsidiaries of the said company all over the world with the aim to defame the company and its Managing Director Mr. R K Malhotra. The plaintiff filed a suit for permanent injunction restraining the defendant from doing his illegal acts of sending derogatory emails to the plaintiff.Onbehalf of the plaintiff, it was contended that the emails sent by the defendant were distinctly obscene, vulgar, abusive, intimidating, humiliating and defamatory in nature. Counsel further argued that the aim of sending the said emails was to malign the high reputation of the plaintiff all over India and the world. He further contended that the acts of the defendant in sending the emails had resulted in an invasion of the legal rights of the plaintiff .Further, the defendant is under a duty not to send the aforesaid emails. It is pertinent to note that after the plaintiff company discovered the said employee could be indulging in the matter of sending abusive emails, the plaintiff terminated the services of the defendant .After hearing detailed arguments of Counsel for Plaintiff, Hon'ble Judge of the Delhi High Court passed an ex-partead interim injunction, observing that a prima facie case had been made out by the plaintiff. Consequently, in this cyber fraud case in India, the Delhi High Court restrained the defendant from sending derogatory, defamatory, obscene, vulgar, humiliating and abusive emails, either to the plaintiff or to its sister subsidiaries all over the world, including their Managing Directors and their Sales and Marketing departments. Further, Hon'ble Judge also restrained the defendant from publishing, transmitting or causing to be published any information in the actual world, as also in cyberspace, which is derogatory or defamatory or abusive.This order of Delhi High Court assumes tremendous significance as this is the first time that an Indian Court assumes jurisdiction in a matter concerning cyber defamation and grants an ex-parteinjunction restraining the defendant from defaming the plaintiff by sending derogatory, defamatory, abusive and obscene emails either to the plaintiffs or their subsidiaries.

3. ONLINE CREDIT CARD FRAUD ON E-BAY

Bhubaneswar: Rourkela police busted a racket involving an online fraud worth Rs 12.5

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1267-1275 www.ijaem.net ISSN: 2395-5252

lakh. The modus operandi of the accused was to hack into the eBay India website and make purchases in the names of credit cardholders. Two persons, including alleged mastermind DebasisPandit, a BCA student, were arrested and forwarded to the court of the subdivisional judicial magistrate, Rourkela. The other arrested person is Rabi Narayan Sahu.Superintendent of police D.S. Kutty said the duo was later remanded in judicial custody but four other persons allegedly involved in the racket were untraceable. A case has been registered against the accused under Sections 420 and 34 of the Indian Penal Code and Section 66 of the IT Act and further investigation is on, he said. While Pandit, son of a retired employee ofRourkela Steel Plant, was arrested from his Sector VII residence last night, Sahu, his associate and aconstable, was nabbed at his house in Uditnagar.Pandit allegedly hacked into the eBay India site and gathered the details of around 700 credit cardholders. He then made purchases by using their passwords. The fraud came to the notice of eBay officials when it was detected that several purchases were made from Rourkela while the customers were based in cities such as Bangalore, Baroda and Jaipur and even London, said V. Naini, deputy manager of eBay.The company brought the **matter to the notice of Rourkela police after some customers lodged complaints.Panditused the address of Sahu for delivery of the purchased goods, said police. The gang was involved in train, flight and hotel reservations. The hand of one Satya Samal, recently arrested in Bangalore, is suspected in the crime. Samalhad booked a room in a Bangalore hotel for three months. The hotel and transport bills rose to Rs 5 lakh, which he did not pay.**

4. **Facebook** :- facebook database leak data of 419 million users[7]**.**Another very prominent attack was on Facebook and Twitter user data. The personal information of around 419 million users was broken to third parties. The Insecure database allowed the hackers to access the phone numbers, user's name, gender, and location of around 419 million users that were linked to their Facebook accounts. Though the attack took place around the geographies, it also included the data of many Indian users. DRI claims Facebook failed to protect user data and notify those who had been affected. The data leak was first discovered and fixed in 2019, but was recently made easily available online for free.DRIsaid individual users who take part in the legal actioncouldbeofferedcompensationofupto €12,000 (£10,445) if it is successful - based on what it says are similar cases in other countries**.** He added: "The laws are there to protect consumers and their personal data and it's time these technology giants wake up to the reality that protection of personal data must be taken seriously."

5.PhishingscamtargetsLioydsBankcustomers :- Customers of Lloyds Bank are being targeted bya phishing scam that is currently hitting email and text message inboxes.Legal firm Griffin Law has alerted people to the scam after being made aware of about 100 people who have received the messages.The email, which looks like official Lloyds Bank correspondence, warns customers that their bank account has been compromised. It reads: "Your Account Banking has been disabled, due to recent activities on your account, we placed a temporary suspension untill [sic] you verify your account."

6. Corona virus now possibly largest ever Cyber Threat security :-

The total volume of phishing emails and other security threats relating to the Covid-19corona virus now represents the largest coalescing of cyber attack types around a single theme that has been seen in a long time, and possibly ever, according to Sherrod DeGrippo, senior director of threat research and detection at Proofpoint.To date, Proof point has observed attacks ranging from credential phishing, malicious attachments and links, business email compromise, fake landing pages, downloader's, spam, and malware and ransomware strains, all being tied to the rapidly spreading corona virus."For more than five weeks, our threat research team has observed numerous Covid-19 malicious email campaigns, with many using fear to try to convince potential victims to click," said DeGrippo.

7. Cosmos Bank Cyber Attack in Pune

A recent cyber attack in India in 2018 was deployed on Cosmos Bank in Pune. This daring attack shook the whole banking sector of India when hackers siphoned off Rs. 94.42 crores from Cosmos Cooperative Bank Ltd. in Pune. Hackers hacked into the bank's ATM server and took details of many visas and rupee debit cardholders. Money was wiped off while hacker gangs from around 28 countries immediately withdrew the amount as soon as they were informed.

8. Social media profile Hacking:- AmitabhBachchan's twitter handle got hacked and the perpetrators posted hateful messagesputting

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1267-1275 www.ijaem.net ISSN: 2395-5252

everybody in shock. This can happen to big companies also. However, if the news gets out this can be a huge blow to the credibility of any company [8].

7. CYBER LAW :-Cyber Law took birth in order to take control over the crimes committed through the internet or the cyberspace or through the uses of computer resources. Description of the lawful issues that are related to the uses of communication or computer technology can be termed as Cyber Law. Cyber law is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e.the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectualproperty, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

8. Importance of Cyber Law :-

Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspective [9].

9. Cyber Law awareness program :- Once should have the following knowledge in order to stay aware about the cyber crime:

- One should read the cyber law thoroughly.
- Basic knowledge of Internet and Internet's security.
- Read cyber crime's cases. By reading those cases one can be aware from such crimes.
- Trusted application from trusted site can be used for protection of one's sensitive information or data.
- Technology's impact on crime.

10. The Information Technology Act of India, 2000 According to Wikipedia "The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an act of the Indian Parliament (no 21 of 2000), it was notified on 17th October 2000. It is the most important law in India that deals with the digital crimes or cyber crimes and electronic commerce. It is based on the United NationsModel Law on Electronic Commerce 1996 (UNCITRAL Model) recommended by the General Assembly of United Nations by a resolution dated 30 January 1997[10].

Some key points of the Information Technology (IT) Act 2000 are as follows:

- E-mail is now considered as a valid and legal form of communication.
- Digital signatures are given legal validity within the Act.
- Act has given birth to new business to companies to issue digital certificates by becoming the Certifying Authorities.
- This Act allows the government to issue notices on internet through e-governance.
- The communication between the companies or between the company and the government can be done through internet.
- Addressing the issue of security is the most important feature of this Act. It introduced the construct of digital signatures that verifies the identity of an individual on internet.
- In case of any harm or loss done to the company by criminals, the Act provides a remedy in the form of money to the company [11].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1267-1275 www.ijaem.net ISSN: 2395-5252

11. Cyber Law in India[12] :-

SECTION	OFFENCE	DESCRIPTION	PENALTY
65	Tampering by computer source records	If a person intentionally hides, destroys or modifiesor purposely or knowingly creates another to screen, destroy or alter any computer source code applied for a computer, computer program, computer operation or computer network, while the computer source code is needed to be stored or supported by law for the time remaining in force	Imprisonment up to three times, or/plus with a fine up to 200,000INR
66	Hacking computer system	If a person including the intention to cause or understanding that he is expected to cause wrongful loss or injury to the public or any person damages or deletes or alters any information remaining in a network resource or decreases its power or utility or affects it seriously by any means performs hack.	Capturing up to three years,/ with fine up to 500,000INR
66B	stolen computer or communication device	A person takes or retains a computer resource or Communicationequipment that is known to be stolen or the person has reason to believe it is stolen	Imprisonment up to three years, or with fine up to 100,000 INR
66 C	Using the password of a different person	A person fraudulently accepts the password, digital sign or other individual identificationofadifferent person.	Isolation up to three years, or with fine up to 100,000INR
66D	Defrauding using computer resource	If a character cheats someone doing a computer resource or information.	Confinement up to three years, or with a fine up to 100,000 INR
66E	Publishing own images of others	If a person takes, transfers or issues images of a person's	Imprisonment up to 3 years, or/and with a fine up to 200,000 INR

		private parts outdoors his/her consent or knowledge	
66F	Laws of cyber terrorism	If a person refuses access to authorized personnel to acomputer device, enters a protected system or introduces contaminant into a system, to advance the unity,integrity, freedom or security of India, then he commits cyber terrorism.	Capturing up to life.
67	Publishing data which is obscene in electronic form.	If a person writes or gives or causes to be published in the electronic form, any material which is obscene or appeals to the prurient interest or if its effect is such as to tend to corrupt and corrupt characters who are likely, having regard to all relevant factors, to read, see or hear the matter included or incorporated in it.	Imprisonment up to five years, or/and with fine up to 1,000,000 INR
67A	Publishing images including sexual acts	If a character publishes or sends images containing a sexually specific act or conduct	arrest up to seven years, or/and with a fine up to 1,000,000 INR
67B	Publishing child porn or predating kids online	If a person captures, distributes or transmits images of a child in a sexually specific act or conduct. If a person induces a child into a sexual act. A child isdescribed as anyone following 18.	Imprisonment up to five years, or with a fine up to 1,000,000 on the first conviction.
67C	Failure to keep records	Persons deemed as an intermediary must maintain required records for a stipulated time. Failure is an offense	Imprisonment up to three years, or with a fine.
68	Failure to comply with orders	The Controller may, by order, designate a Certifying Authority or any employee of such Authoritytoexercise such measures or cease carrying on such activities as defined in the order if those are needed to ensure agreement with the requirements of this Act, rules or any commands made there under. Any person who fails to comply with any such order shall be guilty ofan offense.	Imprisonment up to two years, or with a fine up to 100,000INR

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1267-1275 www.ijaem.net ISSN: 2395-5252

69	Failure to decrypt data	If the Controller is convinced that it is necessary or advisable so to do in the case of the sovereignty or honesty of India, the safety of the State, close relations with international states or public order or for stopping stimulus to the commission of any cognizable crime, for reasons to be reported in writing, by order, direct any agency of the Court to intercept anyinformation conveyed through any computer resource. The patron or any person in charge of the computer store shall when called upon by any agency which has been conducted, must extend all facilities and technical compensation to decrypt the information. The signer or any person who fails to assist the agency referred is deemed to have committed a crime.	Imprisonment up to 7 years and a possible fine.
70	Ensuring accessor striving to secure access to apreserved system	The appropriate Council may, by notification in the Official Gazette, state that anycomputer,computer system or computer network to be a guarded system.	Imprisonment up to 10 years, or with a fine.
71	Misrepresentation	If anyone makes any misrepresentation to or crushes any material fact from, the Controller or the Certifying Authority for receiving any permission or Digital Signature Certificate	Imprisonment up to 2 years, or/and with a fine up to 100,000INR

CONCLUSION: - It can be said that each individual is at risk of cyber crimes, but they all are not victims. Cyber crime is not always related tocomputer only, but is operated through computer networks over the electronic communication channels. It is quite difficult to assess that someone is hacked, whereas, hacking can easily be performed across borders[13]. With the advancement of technology, cyber criminals easily commit crime from their homes. Terrestrial laws may not be sufficient to reduce cyber crimes. Several countries depend upon these laws to conduct legal proceedings. Sometimes, cyber crimemay have huge adverse impact on economic scale. Hence, there is an utmost need to execute huge penalties to reduce rate of such crimes. Further, in this era of advanced technology, users must be made aware about several methods of information security. At the same time, adequate technologies must be developed to address these concerns efficiently. Otherwise, weak technical solutions may worsen the situation. On a global scale, coordinated efforts must be taken to eliminate the gaps between terrestrial laws. This can significantly help to combat cybercrime more easily as similar jurisdictions may streamline the process of fighting against such incidents. It is important to understand the severity and promoting a secure environment while utilizing the technology. Legal and technical resources together may eliminate the complexity. With these approaches,cyber-crimes can be decreased to a greater extent, which may further help in building the progressive economies, offering positive growth environment to business organizations.

REFERENCES:-

[1].https://www.cisco.com/c/dam/en/us/products /collateral/security/2020-outcomes-study-main-report.pdf
[2]. https://www.tutorialspoint.com/information_security_ cyber_law/introduction.htm
[3]. https://cybercrime.org.za/definition
[4].https://www.researchgate.net/publication/303522263
[5]. https://cybercrime.org.za/definition
[6]. https://www.toppr.com/guides/business-laws-cs/cyber-laws/classification-
[7]. https://www.znetlive.com/blog/top-10-cybersecurity-incidents-
[8].https://www.businessinsider.in/tech/news/533-million-facebook-users-
[9].https://www.indiatoday.in/movies/celebrities /story/amitabh-bachchan-t
[10]. http://www.cyberlawsindia.net/cyber-india.html
[11].https://en.wikipedia.org/wiki/Information_Technolo gy_Act,_2000
[12]https://www.ijarcsse.com/docs/papers/Volume_5/8_ August2015/V5I8-0156.pdf
[13]. .https://indiankanoon.org/doc/1439440
[14]. Conclusions Cyber Law | Vulnerability(Computing) | Computer Security(scribd.com)

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 5 May 2021, pp: 1267-1275 www.ijaem.net ISSN: 2395-5252