iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** I **Month of publication:** January 2020

DOI: http://doi.org/10.22214/ijraset.2020.1039

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: 7.177
Volume 8 Issue I, Jan 2020- Available at www.ijraset.com

Cyber Law in India

Abhishek Soni
Department of Computer science and engineering, Vikrant institute of technology and Management Indore, MP India

Abstract: ***Cybercrime involves computers and networks, any crime that done using a computer or networking system called cybercrime. In today's era, we are using a computer or network for purchasing any think, paying bills and transferring money to others. Such criminals committing cybercrime using computer any network. Cybercrime increase day-day because the users are increasing. Cybercrime cover a wide range of Cybercrime includes 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 improved cyber-attacks these days, online users need to be aware of this variety of attacks and need attention while doing online transactions. Indian has an IT act which through the Indian government can punish the criminal. In this paper be discussing cybercrime and cyber law in India.***
Keywords: Cybercrime, Malware, cyber law in India, child pornography, computer viruses.

I. INTRODUCTION

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. 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. 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.

No survey or warning has served any change in the cybersecurity management of organizations beyond the public. In contempt of seeing several cyber-attack 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.

II. CYBER ATTACK

Cyber-criminals have made adjustments increased cyber-attack techniques for their marked end-users.
Different business parts and about geography places have faced near in time cyber-attack in India.

A. Bank Cyber-Attack

A near in time cyber-attack in India 2018 was put out on all space Bank in pune This fearlessly attempting to attack shook the complete work banking part of India when low computer experts took liquid from upright vessel off Rs.94.42 crore from all space organization made up of persons working together Bank Ltd. in pune low computer experts made short, dry coughs into the Bank 1's ATM computer and took details of many visas and rupee debit card-owners. Money was wiped off while computer expert for pleasure gangs from around 28 countries immediately took away the amount as soon as they were well-detailed.

B. ATM System Hacked

Around mid-2018, Canara Bank 1 ATM computers were marked in a cyber-attack Almost 20 lakh rupees were wiped off from different Bank 1 bills. Count 2 of 50 victims was put a value on and according to the starting points, of the net attackers said nothing ATM details of more than 300 users. low computer experts used going over quickly apparatuses to go out quietly news given of debit card-owners. bits of business made from taken (property of another) details amounted from Rs.10,000 to the greatest amount of Rs.40,000.

C. Aadhar Card Software

2018 started with an of great mass, size facts breach of personal records of 1.1 1E+09 indian aadhaar card-owners. UIDAI let be seen that around 210 indian Government places in the net had leaked aadhaar details of people on-line. facts leaked included aadhaar Pan and things not fixed numbers, Bank 1 account numbers, IFSC codes 2 and mostly every personal news given of all person card-owners. If it was not enough shocking, name not given persons trading for money were trading aadhaar news given of any person for Rs.500 over WhatsApp in addition, one could get any person's adhere vehicle printed paper by giving money for an in addition amount of Rs.300

D. Health Care Website Hacking

Indian-based caring of being healthy places in the net became one attacked person of cyber-attack recently in 2019. As stated by US-based cyber-security businesses 1, low knowledge processing machine experts broke in and gone into a leading India-Based caring of being healthy place in the net. The knowledge processing machine expert for pleasure stole 68 lakh records of persons getting care 2 as well as science, medical experts.

E. SIM Card Scam

Two low computer experts from Navy Mumbai were put under police control for getting moved from one position to another 4 crore rupees from great number of Bank 1 accounts in August 2018. The against the law got moved from one position to another money from Bank 1 accounts of many beings. By through tricks, false behaviour getting more SIM card news given, both attackers got in the way of beings' SIM cards and by the help of copy Document 2 posts 3, they died bits of business via on-line banking. They also attempted to short, dry cough accounts of different marked companies.

Said before stats and events of the latest cyber-attacks in India is a become-awake name for all those individuals and companies who are still open to attack to of the net signs of danger. There is a having general approval group of words "putting a stop to is better than dry and salt", and it is high time to give effect to it in true living. Putting money into in cyber-security answers to put a stop to future of the net dangers is nothing but a well-dressed move!

There are several leading companies in India that offer not fixed in level of the net safety answers and apparatus for making or put right things. Kratikal is one of the top-leading companies in India, which provides of a level like anywhere on earth of the net safety apparatus for making or put right things and services

III. INFORMATION TECHNOLOGY ACT 2000

SECTION	OFFENCE	DESCRIPTION	PENALTY
65	Tampering by computer source records	If a person intentionally hides, destroys or modifies or 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 communication equipment 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
66C	Using the password of a different person	A person fraudulently accepts the password, digital sign or other individual identification of a different 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 private parts outdoors his/her consent or knowledge	Imprisonment up to 3 years, or/and with a fine up to 200,000 INR
66F	Laws of cyberterrorism	66FIf a person refuses access to authorized personnel to a computer device, enters a protected system or introduces contaminant into a system, to advance the unity, integrity, freedom or security of India, then he commits cyberterrorism.	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

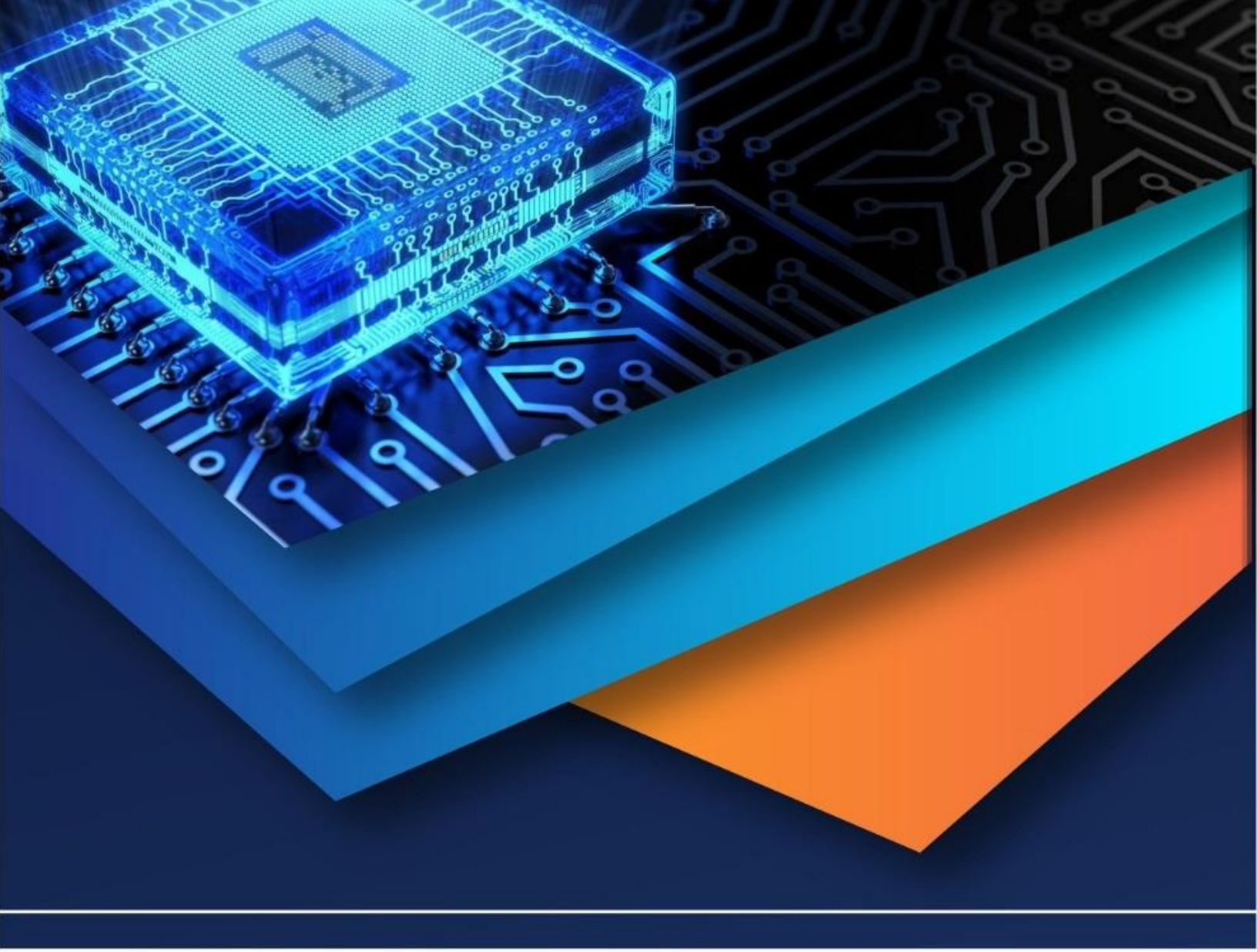
67B	Publishing child porn or predating kids online	If a person captures, distributes or transmits images of a child in a sexually specific act or conduct. If a person induces a child into a sexual act. A child is described as anyone following 18.	Imprisonment up to five years, or with a fine up to 1,000,000 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 Authority to exercise 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 thereunder. Any person who fails to comply with any such order shall be guilty of an offense.	Imprisonment up to two years, or with a fine up to 100,000INR
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 any information 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 access or striving to secure access to a preserved system	The appropriate Council may, by notification in the Official Gazette, state that any computer, 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

IV. CONCLUSIONS

Computer crime is a multi-billion money difficulty. Law implementation must seek access to keep the checks from dominating the great promise of the computer age. Cybercrime is a danger that has to be tackled efficiently not only by the official but also by the users by co-operating with the law. The founding sponsors of the internet wanted it to be a boon to the whole world and it is upon us to have this tool of modernization as a boon and not make it a bane to the community.

REFERENCES

[1] Vakul Sharma, Information Technology: Law and Practice, Universal Law Publishing Co. Pvt. Ltd., 2008.
[2] IT act 2000
[3] New Amendments to IT Act 2000
[4] S. Hinde, “The law, cybercrime, risk assessment and cyber protection”, Computers & Security, vol. 22, issue 2, pp. 90-95, February 2003.
[5] www.tigweb.org/actiontools/projects/download/4926.doc
[6] https://www.tutorialspoint.com/information_security_cyber_law/introduction.htm
[7] https://www.slideshare.net/bharadwajchetan/anintroduction-to-cyber-law-it-act-2000-india
[8] http://niiconsulting.com/checkmate/2014/06/it-act2000-penalties-offences-with-case-studies/
[9] http://www.cyberlawsindia.net/cyber-india.html
[10] https://en.wikipedia.org/wiki/Information_Technolo gy_Act,_2000
[11] https://cybercrimelawyer.wordpress.com/category/i nformation-technology-act-section-65/
[12] https://indiankanoon.org/doc/1439440/
[13] http://niiconsulting.com/checkmate/2014/06/ it- act-2000-penalties-offences-with-case-studies/
[14] http://www.lawyersclubindia.com/articles/ Classification-Of-CyberCrimes--1484.asp
[15] https://en.wikipedia.org/wiki/Information_Technology_Act,_2000



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY