iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** II **Month of publication:** February 2022

DOI: https://doi.org/10.22214/ijraset.2022.40213

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: 7.538
Volume 10 Issue II Feb 2022- Available at www.ijraset.com

A Study on Types of Cyber Crimes and Cyber Attacks Today

Anushka Alok Lodh[1], Chetan Vijaykumar Dalave[2]
[1, 2]*Dept.Of Computer Engineering Savitribai Phule Pune University, RMD Sinhgad College of Engineering Pune, Maharashtra, India*

Abstract: ***With the increasing number of COVID-19 cases in the world and deaths worldwide has given a very worse condition to the whole world besides this covid pandemic there is also increase in number of Cyber-crimes and Cyber-attack of different types in the whole world. As Technology is advancing everyday there is a rise in Cyber-crime problem today, however security measures and prevention to protect this technology and the users of the technology is not advancing as quickly. So, the aim of this study is to understand and learn different types of Cybercrimes and Cyberattacks today in the world. It is important to prevent and to put awareness about the types of crimes and attacks. There are some protective procedures such as keep your software Up to date, Using of Anti-Virus Protection and also the use of Firewall, Continuously Changing Passwords and keep it as strong as can be, and also two step or multi step authentication should be done whenever necessary.***
Keywords: Cyber-crimes, Cyber-attacks, Types of Cyber-crimes, Prevention Measures, Threats.

I. INTRODUCTION

Cybercrime and cyberattack is the action that aims and uses a computer network, computer or any of the network device using all this harms or damages the organizations or person's data or information and use it in the wrong way. All this malicious act is carried out by cybercriminals or hackers or any individual Cybercrime Organization, the aim of this Organization or Cybercriminals is to break the CIA Triad i.e., Confidentiality, Integrity and Availability of data. Because of todays digitalized and technologies-based environment, the world is becoming more and more sophisticated digitally and also sophisticated with internet connections so are the crimes are also increasing day by day. Increasing Crimes and attacks Forced government to make a Cyber Law so there is a need of Cyber law which will protect, prevent and give the safeguard to the data and information of an organization or of an individual. At that time the IT Act was established i.e. The Information Technology Act, 2000, also known as the IT Act, was enacted by the Indian Parliament on 17 October 2000. The Information Technology Act is based on the United Nations Electronic Commerce Model Act 1996 (UNCITRAL Model), which was proposed by the United Nations General Assembly in a resolution dated January 30, 1997. It is most vital law in India dealing with Cybercrimes and Attacks. The main determination of this act is to convey legal and honest electronic, digital and online transaction and give relieve or reduce cybercrimes. As COVID-19 increased and today everything done by online mode only there is an advantage to the hackers and cyber criminals as they are threating and attacking on the any global organization, a computer network or any system of an individual, and also the businesses at a time when cyber defenses might be lowered due the all focus on health crisis. Most of the Attacks like Malicious domains, Malware and Ransomware is going on and on during these days.

II. LITERATURE SURVEY

SR. NO	Paper Title/Publication details	Pre-Processing	Feature Extraction and Classification	Accuracy	Post-Processing
1.	"Covid-19 Pandemic: A New Era of Cyber Security Threat and Holistic Approach to Overcome. Ahmed and Q. Tushar *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, 2020, pp. 1-5, doi: 10.1109/CSDE50874.2020.9411533.	Studied on the threats and the prevention that should be done to stop these crimes.	NCSC, CISA, DDoS Focusing on some of the safety prevention to prevent the personal and organizational data from the cyber criminals	85%	This survey shows threat to cybersecurity around the world in the present situation of this COVID -19 pandemic, also shows safeguard that should be taken to reduce cybercrimes.
2.	Predicting and Preventing Cyber Attacks During COVID-19 Time Using Data Analysis and Proposed Secure IoT layered Model," L.	To analyze data that is related to phishing attacks using	We analyzed about neural networks that collects the data about phishing attack to		Will do a survey on the nature of the cyberattacks which is the outbreak of COVID-19

	Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider and G. Saldamli, *2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA)*, 2020, pp. 113-118, doi: 10.1109/MCNA50957.2020.9264301.	the neural networks, it will also cover some of the social and economic aspects.	understand better trends and reduce attacks.	89%	pandemic.
3.	"A Study on Various Cyber Attacks and A Proposed Intelligent System for Monitoring Such Attacks," A. S. Choudhary, P. P. Choudhary and S. Salve, 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 612-617, doi: 10.1109/ICICT43934.2018.9034445.	Many systems and websites were hacked in the past few years and has caused a huge loss to nations and it need a prevention i.e., machine learning.	Reported Proposed intelligent system that is supervised and Techniques for learning to avoid these cyber attacks	77%	It presents a study on paper Numerous cyber-attacks that started in India. Countries in the last few years.
4.	"Investigation and classification of cyber-crimes through IDS and SVM algorithm," H. Zolfi, H. Ghorbani and M. H. Ahmadzadegan, 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 180-187, doi: 10.1109/I-SMAC47947.2019.9032536.	As Cybercrimes has been increased there is need to detect those crimes using different techniques	The present study investigates computer crime. Through a petrochemical traffic network Through a subsidiary within a specified period of time Modeling attacks using SVM algorithm.	85%	To identify meaningful pattern to categorize attacks as a solution to detect as much as malicious attacks and prevent future criminal activities with the help of intrusion detection system.
5.	"Thwarting Cyber Crime and Phishing Attacks with Machine Learning: A Study," M. Arshey and K. S. Angel Viji, 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, pp. 353-357, doi: 10.1109/ICACCS51430.2021.9441925.	Focuses on different types and targets of cybercrime. Some of today's cybercrime attacks are based on phishing, Artificial intelligence, cloud technology and blockchain.	Different machine learning models Expecting, identifying and justifying complex threats Is also under discussion.	76%	This survey aims to categorize machine learning. Learning can be deployed in exploring diverse areas of cyber. Crime
6.	"An Empirical Study of Cybercrime and Its Preventions," S. Batra, M. Gupta, J. Singh, D. Srivastava and I. Aggarwal, 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2020, pp. 42-46, doi: 10.1109/PDGC50313.2020.9315785.	Will have analyse statistical data on different types of cybercrime and it grew in last few years.	Cybercrime happens fast and fetch one of the highest rising forms of present crime. Cybercrime is known for its decline. Companies, organizations and personal identities.	73%	To define cybercrime, different types cybercriminals that affect the world also its Prevention.
7.	,"A Technical Review Report on Cyber Crimes in India," P. Datta, S. N. Panda, S. Tanwar and R. K. Kaushal, 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), 2020, pp. 269-275, doi: 10.1109/ESCI48226.2020.9167567.	This review has been thoroughly reviewed Cybercrime in India.	To reduce cybercrime, more secure, Efficient technology and networking systems are desired. Designed and applied to secure important personal data.	87%	This study shows that how fraud cases are increasing, and peoples those are affected are women's and children.
8.	"Classification and Imapct of Cyber Threats in India: A review," S. Tanwar, T. Paul, K. Singh, M. Joshi and A. Rana, 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020, pp. 129-135, doi: 10.1109/ICRITO48877.2020.9198024.	This paper tries to process about the different classifications of crimes and its prevention.	This review pays attention to the serious matter which is just, Growing over time. The article describes various crimes. Potential threats to a user on the Internet and The cyber world	68%	This paper Compares previously written data and information. Research papers on this issue.
9.	"A Survey on Cyber Security Threats and Challenges in Modem Society," S. Z. Sajal, I. Jahan and K. E. Nygard, 2019 IEEE International Conference on Electro Information Technology (EIT), 2019, pp. 525-528, doi: 10.1109/EIT.2019.8833829.	As the cybercrimes are not in the specific firm area. There is a need of solution that will reduce crime from India.	To deal with maximum security threats there are solutions to those threat.	78%	This study presents the tasks and threats that makes the system weak,

10.	Cyber Crime in India: An Empirical Study Prof. Saquib Ahmad Khan International Journal of Scientific & Engineering Research Volume 11, Issue 5, May-2020 ISSN 2229-551	Previously it was studied by authors that how the law came which precaution should be taken for different types of attacks and crimes, and which methodology is required for securing the data.	With the increasing number of crimes there is cyber law developed by government of India, which deals with technology and also punishes for computer crimes.	86%	we will discuss about the common types and its prevention to prevent cybercrimes.
11.	Cyber Crimes in India: Trend and Preventions Sanjeev Kumar, Dr Anupam Manhas GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ) ISSN (E): 2347-6915 Vol. 9, Issue 5, May (2021)	Previously government is issuing an advisory to the general public not to fall prey to it. These are just crimes and be careful when entering your details and passwords on online sites.	Psychological, physical, sexual or as a result of cyber violence, economic loss to women. In between March and April 2020, India grew by a shocked 86% Cyber-attacks.	72%	This study objects to examine the growing number of cyber cases. Violations, amid the urgent need for more strong and complete cyber security measures.
12.	A Study on Cyber Crime and its Legal Framework in India APOORVA BHANGLA1 AND JAHANVI TULI Vol.no 4 2021. International Journal of Law Management & Humanities [ISSN 2581-5369	Different Section has been passed by the law to punish the criminal for cybercrime.	Cyber Pornography, IAMAI, IPC and IT Act, Anonymity, ISPs	68%	This studies aim is to study cybercrimes and Its framework in India.
13.	CYBER CRIMES IN INDIA: TRENDS AND PREVENTION Ms. Riddhi Shah 2019 IJRAR March 2019, Volume 6, Issue 1	Data analyzation and data collection is done previously to show the number of crimes its prevention and also the section of laws by government of India.	NCRB, IPC, NITI, DSCI, NASSCOM, CERT-In, IAMAI, IMRB I, CUBE	71%	This study focuses on the growing trends in Internet usage and the risks facing consumers in India. Also, to study cyber- crime reporting trends in India
14.	RESEARCH PAPER ON CYBER SECURITY Mrs. Ashwini Sheth1, Mr. Sachin Bhosale2, Mr. Farish Kurupkar CONTEMPORARY RESEARCH IN INDIA (ISSN 2231-2137): SPECIAL ISSUE: APRIL, 2021.	How can you recognize, protect? Organizations, threats notice and response, and Make the most of successful events.	DNS, AIC, CIA, DoC.	81%	The purpose of this is to identify the types of threats and find the related ups and downs that might the result.

A. Types of Cyber Crimes and Cyber Attacks

1) *Phishing*- Phishing is a form of fraud that involves stealing information about your banking account card details E-mail.
2) *Hacking*- Hacking refers to activities that may attempt to break into a computer network through unauthorized access, including Inserting malicious content on your device (computer, laptop, smartphone, tablet). One more type of hacking is Hacktivists are identified as politically inspired hacktivists. White hat, gray hat and white hat are hackers.
3) *Intellectual Property Crimes*- Also recognized as IPR, intellectual property rights consist of many rights, with IPR. Copyright, patents, trademarks, trade secrets. Intellectual property law inspires inclusive-ranging formation and safety. Mutual types of intellectual property rights violations are also fake, piracy-breach. This includes theft works of art and literature and designs.
4) *Spreading Virus*- Viruses are lists that attach themselves to a computer and can mix inside the computer. These viruses can copy information from under siege computer systems and use it for various illegal purposes. There are various kinds of viruses, stealth viruses, polymorphic viruses, fast and slow infecting.
5) *Carding*- This is a type of fraud that uses stolen credit cards to pay for criminal or illegal activities. Without the knowledge of the credit card owner, it is also known as credit card smuggling.
6) *Vishing (Voice Phishing)*- Banking account card information is obtained by fraudsters using telephonic way.

7) *Cyber stalking* - In general, cyber stalling means the use of digital systems of computer systems and communications Even after a clear message of disinterest from a person trying to continue a personal interaction, Online harassment, slander, slander is included.
8) *Internet Time Thefts*- Internet time theft is another type of hacking in which a hacker gains access to your Internet services and the identity password for it without the knowledge of the person who pays for these internet hours.
9) *Cracking*- In general, cracking means stealing data, hacking into a computer to view sensitive information. A cracker is different from a hacker because it uses a backdoor in a program and then uses that backdoor to gain access on the other side hacker uses wide computer information and logic to avoid security.
10) *E-Mail/SMS Spoofing*- Email spoofing is an email that is sent through an address that is not valid or is false under the pretext. Someone else (fake), then this e-mail is used to mislead the recipient or to make false statements and dig information.
11) *Cyber Squatting*- This is an attempt to use an Internet domain name, or to use a brand name to its advantage of personal benefit. This is an attempt to represent a brand online without permission or consent.
12) *Key Logger*- It is a criminal act in which an individual's keyboard activity is recorded without his permission and awareness.
13) *Online Job Fraud*- It is an attempt to cheat people with false claim of providing employment with salaries using Internet resources.
14) *Website Defacement*- It is a Type of crime that changes the graphics of the website and do the post of images and messages which are vulgar in behaviour.

B. *Types of Cyber Crimes and Attacks happen during COVID-19*

1) *Phishing of Emails* - It is likely that phishing emails are on the growth. Cyber bullying actors will use COVID-19 phishing emails in an attempt to convince the recipient that they are either sensitive information (i.e., bank account information). Show, or just try to persuade the recipient to open a malicious link or attachment, potentially allowing them access to your system.

Phishing of Emails in issue to COVID-19 may contain issues such as:

a) Vaccine registration
b) Information about your vaccine coverage
c) Places where the people get the vaccines.
d) Ways you can save the vaccine.
e) Vaccine requirements

2) *Ransomware*

a) Much of this is ransomware, a complicated attack on an organization's data and systems. Meanwhile in the beginning of the pandemic, ransomware attacks had increased near to 500% since the occurrence of the COVID-19 pandemic.
b) What is particularly ridiculous about these attacks is that ransom demands often accompany the breach and extraction of company data, and simultaneous extortion threatens to release this data unless that no extra payment be made.

3) *Malware* - During this pandemic, Cybercriminals are spreading malware on devices. Criminals can create malware backdoor in user's devices through which cyber criminals take all personal credentials, passwords and all this is spreading by some online corona tracing maps.
4) *Malicious Fields* - Taking advantages of the rising demand for medical kit and data on COVID-19, there has been a major increase in cybercriminals registration domain names comprising keywords like "Corona Virus" or "COVID". These fake websites sponsor a different type of malicious activities, distribution of malware and phishing. From February to March 2020, malicious registrations, together with malware and phishing, increased by 569%, and high-risk registrations increased by 788%. Noticed with the help of private sector partner and also get reported.
5) *Misinformation* - The increasing amount of misinformation and fake news is spreading among the people. Unproven data, unsatisfactory alleged threats, and plan theories have formed unrest in groups and, in some cases, simplified cyber-attacks. About 30% of the countries that response to the worldwide cybercrime review confirmed the motion of false information about COVID-19.Within a month, one country reported 290 postings, maximum of which carried secreted malware. There are also reports of incorrect information being allied to the illegal trade in fake medical products. Other cases of misinformation contain scams via mobile text messages, with offers such as free food, special aids, or huge discounts in superstores being 'It's great to be honest'.

C. Precautions from Cybercrimes and Attacks during COVID-19 Pandemic

1) Prevention from Phishing of Emails

a) Under how the Phishing scam looks like.
b) Don't click any link in the Email, and must install firewall.
c) Should get free anti-phishing add-ons.
d) Do not put your personal information to any unknown website.

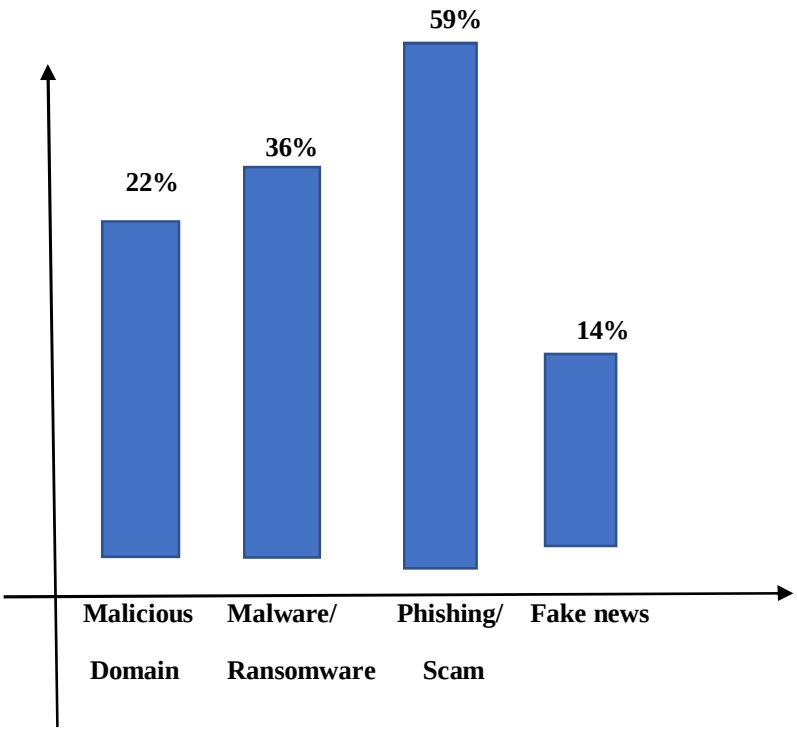
2) Prevention from Ransomware

a) Avoid opening suspicious attachments.
b) Keep your software up-to-date.
c) Have Windows Firewall on at all times and properly organized.
d) Use strong spam filters and verify users.

3) Prevention from Malware

a) Try to use endpoint security tool and network, also installation of anti-virus or anti-malware software and also the firewall.
b) Make use of encryption technique to secure the data during transport.
c) Make proper use of Secure Authentication Methods.

D. Analysis of Cybercrimes and Attacks during Pandemic



IV. CONCLUSIONS

This study seeks to focus on current cyber threats COVID-19 among pandemics. This pandemic has seen maximum Internet usage. People from all parts of the world continued its communication, jobs and education with the help of internet. This pandemic has also given pressure, stress to all stages. With the help of internet stress is being reduced among the peoples at many levels. This pandemic has proved people can work, continue classes and all other activities by staying at home. Cybercriminals have taken advantage of this opportunity, taken advantage of this extensive use of the Internet by large numbers of people. Cyber security threats have increased a lot during these pandemics due to cyber unawareness Information of security. At every level, we should have a least knowledge of cyber security threats and possible cyber-attacks. Most of the affected area are Organization, Government and also non-government fields. Therefore, it is necessary to provide minimum knowledge on cyber security to save every employee from significant loss Information to cyber criminals. COVID-19 is just beginning.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

As we studied how these cybercrimes are affecting the whole world, the world may face such crimes attacks and problems in upcoming future. So, we have to plan for our future to fight with such attacks. We should all learn from this COVID-19 pandemics and can prepare themselves for its Cyber security should not be a problem in the future for the world.

REFERENCES

[1] J. Ahmed and Q. Tushar, "Covid-19 Pandemic: A New Era of Cyber Security Threat and Holistic Approach to Overcome," 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE), 2020, pp. 1-5, doi: 10.1109/CSDE50874.2020.9411533.

[2] L. Tawalbeh, F. Muheidat, M. Tawalbeh, M. Quwaider and G. Saldamli, "Predicting and Preventing Cyber Attacks During COVID-19 Time Using Data Analysis and Proposed Secure IoT layered Model," 2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA), 2020, pp. 113-118, doi: 10.1109/MCNA50957.2020.9264301

[3] S. Choudhary, P. P. Choudhary and S. Salve, "A Study on Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks," 2018 3rd International Conference on Inventive Computation Technologies (ICICT), 2018, pp. 612-617, doi: 10.1109/ICICT43934.2018.9034445.

[4] H. Zolfi, H. Ghorbani and M. H. Ahmadzadegan, "Investigation and classification of cyber-crimes through IDS and SVM algorithm," 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, pp. 180-187, doi: 10.1109/I-SMAC47947.2019.9032536.

[5] M. Arshey and K. S. Angel Viji, "Thwarting Cyber Crime and Phishing Attacks with Machine Learning: A Study," 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021, pp. 353-357, doi: 10.1109/ICACCS51430.2021.9441925.

[6] S. Batra, M. Gupta, J. Singh, D. Srivastava and I. Aggarwal, "An Empirical Study of Cybercrime and Its Preventions," 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2020, pp. 42-46, doi: 10.1109/PDGC50313.2020.9315785.

[7] P. Datta, S. N. Panda, S. Tanwar and R. K. Kaushal, "A Technical Review Report on Cyber Crimes in India," 2020 International Conference on Emerging Smart Computing and Informatics (ESCI), 2020, pp. 269-275, doi: 10.1109/ESCI48226.2020.9167567.

[8] S. Tanwar, T. Paul, K. Singh, M. Joshi and A. Rana, "Classification and Imapct of Cyber Threats in India: A review," 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020, pp. 129-135, doi: 10.1109/ICRITO48877.2020.9198024.

[9] S. Z. Sajal, I. Jahan and K. E. Nygard, "A Survey on Cyber Security Threats and Challenges in Modem Society," 2019 IEEE International Conference on Electro Information Technology (EIT), 2019, pp. 525-528, doi: 10.1109/EIT.2019.8833829.

[10] Cyber Crime in India: An Empirical Study Prof. Saquib Ahmad Khan International Journal of Scientific & Engineering Research Volume 11, Issue 5, May-2020 ISSN 2229-551

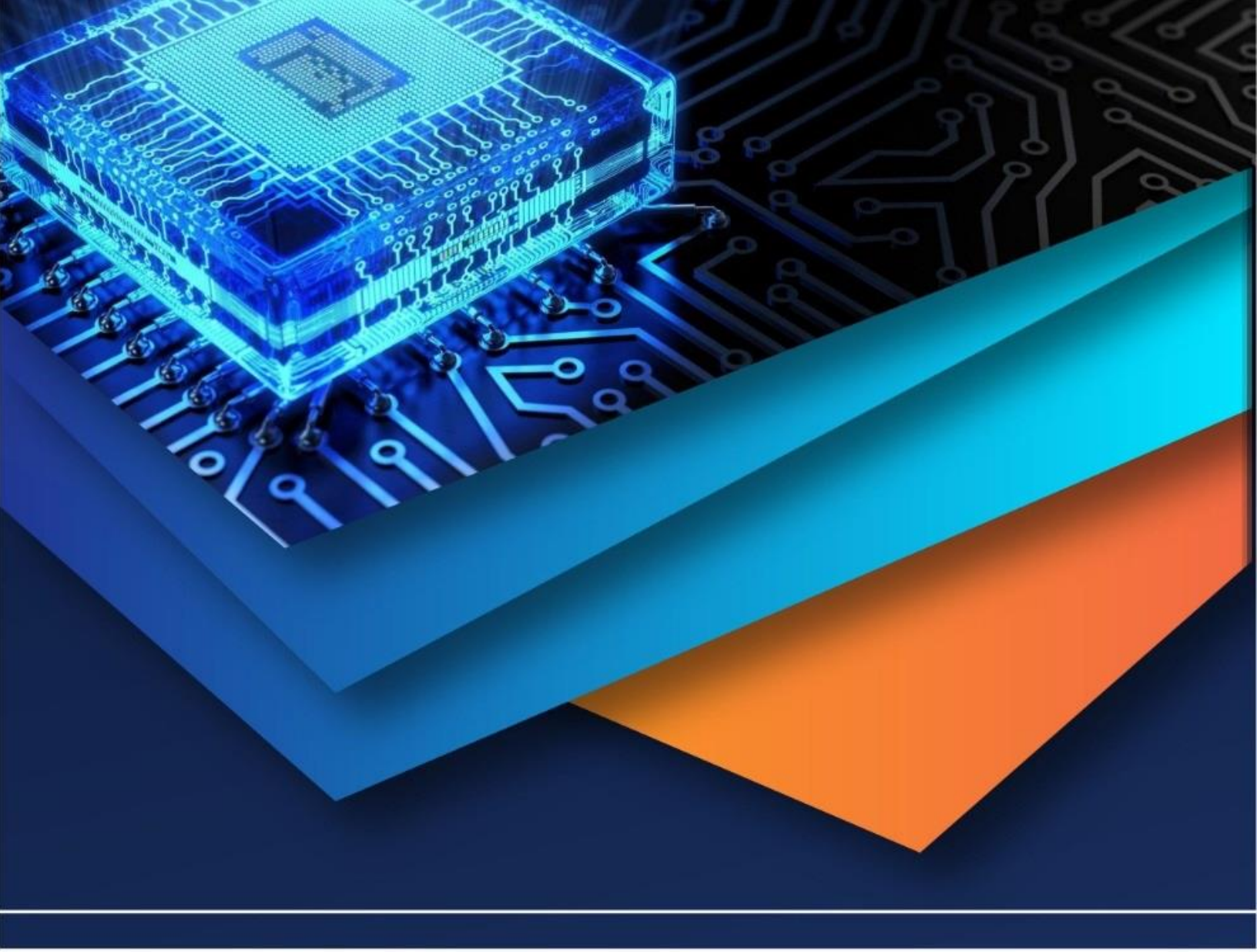
[11] Cyber Crimes in India: Trend and Preventions Sanjeev Kumar, Dr Anupam Manhas GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ) ISSN (E): 2347-6915 Vol. 9, Issue 5, May (2021)

[12] A Study on Cyber Crime and its Legal Framework in India APOORVA BHANGLA1 AND JAHANVI TULI Vol.no 4 2021. International Journal of Law Management & Humanities [ISSN 2581-5369

[13] CYBER CRIMES IN INDIA: TRENDS AND PREVENTION Ms. Riddhi Shah 2019 IJRAR March 2019, Volume 6, Issue 1.

[14] RESEARCH PAPER ON CYBER SECURITY Mrs. Ashwini Sheth1, Mr. Sachin Bhosale2 , Mr. Farish Kurupkar CONTEMPORARY RESEARCH IN INDIA (ISSN 2231-2137): SPECIAL ISSUE : APRIL, 2021.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)