iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XI **Month of publication:** November 2023

DOI: https://doi.org/10.22214/ijraset.2023.57092

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 11 Issue XI Nov 2023- Available at www.ijraset.com

State of the Art - Cybercrimes and Cyber Security Policies and Countermeasures

Anusha A. K. R. S.
Department of Computer Applications, American College, India

Abstract: ***The world has become a global village because of the availability of Internet Connectivity and mobile devices to most of the masses around the world. The benefits of digitalization goes hand in hand with a steep rise in cybercrimes, cyber threats and cyberattacks. Cyber security has become crucial in our day to day life in order to protect our information systems. Cyber security has become a buzz word and has kindled interests among cyber security experts, researchers, academicians, private organizations and the government alike. This paper explores the state of the art in Cyber Security and the challenges caused by cybercrimes, cyber threats and cyberattacks. Various methods to protect individuals, organizations, and governments from cybercrimes has been addressed in this paper. Importantly, ways to detect and report cybercrimes are also dealt with.***
Keywords: Cybercrime, Cyber threat, Cyberattack, Cyber warfare, Cyber Security.

I. INTRODUCTION

1) *Cyber* is a term related to computing, including storing data, accessing data, processing data, protecting data and transmitting data.
2) *Crime* refers to an illegal action which constitutes an offence and is punishable by law.
3) *Cybercrime* is a well-planned, organized, and professional criminal activity including theft, fraud, forgery, and defamation that involves using a computer, a networked device, a network or the Internet to carry out a crime or to be the target of the crime. Cybercrimes breach security and financial health of people or government.
4) *Cybercriminals* are individuals or groups of persons who use technology hack and infiltrate digital systems or networks with malicious intent in order to generate profit.

II. CYBERCRIME

A. *Reasons for Cybercrimes*

1) Desire of making quick money
2) Negligence
3) System vulnerabilities
4) Accessibility to victims online
5) Confidential Information is Online
6) Disgruntled employees
7) Passion for Publicity
8) Loopholes in Judiciary System
9) Lack of Evidence

B. *Types of Cybercrime*

Common Cybercrimes include:

1) *Identity Theft* is a cyber-crime in which a criminal accesses data about an individual's bank accounts, debit cards, credit cards, and other sensitive information to siphon money or to buy things online in the victim's name.
2) *Cyber Stalking* is a kind of online harassment wherein the victim is bombarded with online messages and emails.
3) *Sexting* is an act of sending sexually explicit digital images, videos, text messages, or emails, usually by cell phone.
4) *Online Sextortion* occurs when someone threatens to distribute private and sensitive material using an electronic medium if he/ she doesn't provide images of a sexual nature, sexual favors, or money.
5) *Cyber Grooming* is a cybercrime in which a person builds an online relationship with a young person and tricks or pressures him/ her into doing a sexual act.

6) *Child pornography and Abuse* is a type of cyber-crime wherein criminals solicit minors via chat rooms for the purpose of child pornography.
7) *Dark Web / Online Drug Trafficking* is a type of crime in which a criminal sells illegal weapons, drugs, smuggled goods, or personal information to a person on a prohibited online shopping platform using cryptocurrency. It promotes terrorism and black marketing.
8) *Espionage* refers to monitoring other countries to steal secrets. In cyber warfare, this can involve using botnets or spear phishing attacks to compromise sensitive computer systems before exfiltration of sensitive information.
9) *Cyber Terrorism* refers to unlawful and politically motivated attacks using the Internet to force or compel a government or its people for political or social gains.

III. CYBER ATTACK

A. Cyber Attack

A *cyber-attack* is an exploitation of computer systems and networks by cybercriminals, hackers or other digital adversaries to gain unauthorized access to a computer network or system, usually for the purpose of theft, disruption, altering, destroying or exposing information. The victims of cyberattacks may be individual users, business enterprises, or governments.

B. Common Types of Cyber Attacks

1) *Phishing* is a cyberattack that uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information such as passwords or account number or to download a malicious file that will install viruses on their computer or phone by sending fraudulent communications that appear to come from a reputable source.

Common phishing examples in the COVID era

- Impersonating a doctor and claiming to be able to treat or cure COVID-19.
- Impersonating a government organization that is sharing important public health information.
- Impersonating a courier service that is attempting to deliver a package.

2) *Vishing* is a type of cyberattack where fraudsters try to seek personal information like Customer ID, Net Banking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call.
3) *Smishing* is a type of fraud that uses mobile phone text messages to entice victims into calling back on a fraudulent phone number, visiting fraudulent websites, or downloading malicious content via phone or web.
4) *Pharming* is a cyber-attack aiming to redirect a website's traffic to another bogus website.

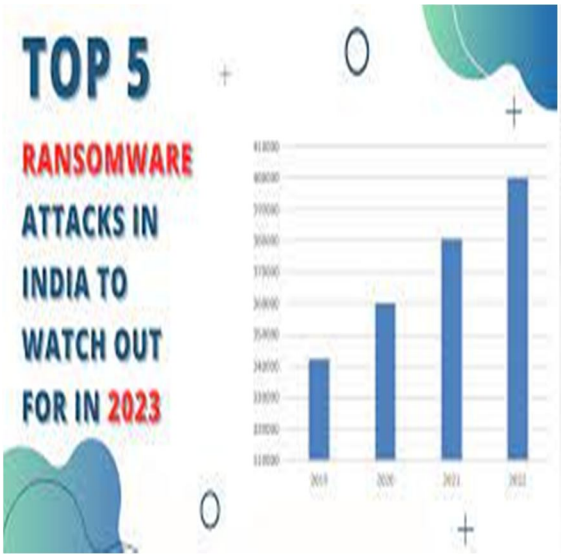


Fig. 1 Ransomware Attacks in India

Fig. 2 Cybercrimes against Women in India

5) *Denial of Services (DoS) Attack* floods systems, servers, or networks with traffic to drain resources and bandwidth making it unable to fulfill legitimate requests.
6) *Distributed Denial of Service (DDoS) Attack* is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. DDoS attacks are launched from multiple systems. Example**:** The AWS DDoS Attack in 2020 on Amazon Web Services (AWS). The AWS DDoS attack, which lasted three days, caused significant revenue losses for AWS customers and reputational harm to AWS.
7) *Password Attack* attempts to steal a user's password. Attackers can use Dictionary Attacks, Password Sniffers, or even Cracking Programs to steal passwords. These attacks aim to accessing passwords that are exported or stored in a file. Cybercriminals can exploit password vulnerabilities if users do not set strong passwords, reuse existing passwords across multiple sites, or fail to regularly change their password.
8) *Eavesdropping* begins with the interception of network traffic in order to steal information that computers, smartphones, or other devices receive or send.
9) *Man-in-the-middle Attack* occurs when attackers eavesdrop on the communication between two entities such as a network user and a web application to collect personal data, passwords or banking details. This type of cybercrime harms both the communicating parties as the attacker can do anything with the interpreted information.

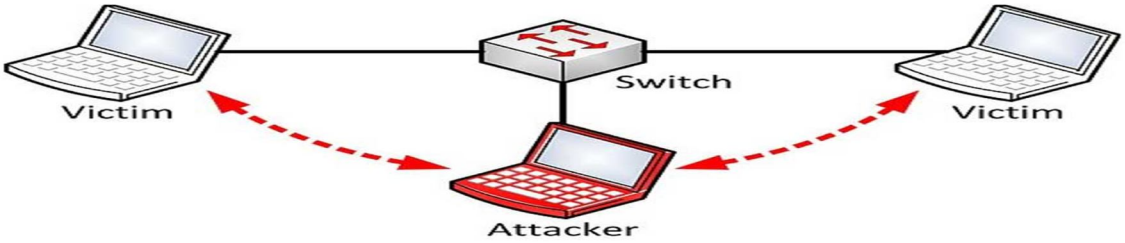


Fig. 3 Man-in-the-Middle Attack

10) *Replay Attack* occurs when an attacker intercepts and saves old messages and then tries to send them later, impersonating one of the participants to produce an unauthorized effect. This type can be easily thwarted using session timestamps or nonce.
11) *IoT Attack* is a cyberattack that targets an Internet of Things (IoT) device or network. If the attack is successful, the hacker gains full control of the device and can steal data, or carry out DoS or DDoS attacks.
12) *AI Powered Attack* uses Artificial Intelligence and Machine Learning to hack many systems, including autonomous drones and vehicles, and convert them into potentially dangerous weapons. The AI-powered applications can be used for performing cybercrimes such as Password Cracking, Identity Theft etc.
13) *Bot Attack* uses a robot for cyberattacks. A bot is short for "robot". A bot is an automated process that can either run automatically or execute commands when they receive specific input. Common examples of bot programs include web crawler (spider), chatbots (perform authentication and authorization), and malicious bots.
14) *SQL Injection Attack* occurs when an attacker inserts malicious SQL statements into a data-driven application which then allows the hacker to steal, alter, or erase information from the database. One of the most common targets of SQL injection attacks are gamers and the gaming industry.
15) *Cross Site Scripting (XSS) Attack* is a code injection attack in which an adversary inserts malicious code within a legitimate website. XSS is a client-side susceptibility that targets other people who visit infected websites. When the users visit the infected web pages the script code is executed in the browser which can be used to steal sensitive data like username and pass word.
16) *Birthday Attack* is used against hash algorithms that are used to verify the integrity of a message, software or digital signature. A message processed by a hash function produces a message digest (MD) or hash code of fixed length, independent of the length of the input message; this message digest uniquely characterizes the message. The birthday attack refers to the probability of finding two random messages that generate the same message digest when processed by a hash function. If the attack is successful, the hacker can safely replace the user's message with his message without getting detected by the receiver.
17) *Sabotage Attack* involves hostile governments or terrorists stealing sensitive information, destroying it, or influencing insider threats such as dissatisfied or careless employees, or government employees with affiliation to the attacking country.

18) *Web Defacement Attack* includes penetration of websites by malicious parties and replacing content on the site with their own information.
19) *Propaganda Attack* aims at exposing embarrassing truths, spreading lies with the intention of making people lose trust in their country, or side with their enemies.
20) *Economic Disruption Attack* involves attackers targeting computer networks of economic establishments such as *stock markets*, *banks*, and *payment systems* to steal money or block people from accessing the funds they need.
21) *Electrical Power Grid Attack* allows attackers to disable critical systems, disrupt infrastructure and communications, and potentially result in bodily harm.
22) *Surprise Attack* targets an enemy when the enemy isn't expecting, enabling the attacker to weaken their defenses.

IV. TOOLS FOR CYBERCRIMES

Malware or malicious software is a software that is developed with the intention of causing harm to a computer, network, or server. Malware includes viruses, worms, ransomware, spyware, Trojans, keyloggers, bots, cryptojacking etc.

1) *Viruses* are programs that infect applications attaching themselves to executable code or the initialization sequence. The virus creates copies of itself, infecting other software in the computer system.
2) *Worms* are self-contained programs that propagate across networks and computers. Worms often spread through email attachments. They send a copy of themselves to every email in the mailing list of the infected computer. They are commonly used to carry out denial-of-service attack by overloading an email server. Worms do not attack the host.
3) *Trojan Horse* is a non-replicating program hiding inside a useful program with malicious purposes. It appears to be a useful program and when executed, causes loss or theft of data and possible system harm.
4) *Logic bomb* is a piece of code intentionally inserted into a legitimate software system that will set off a malicious function when specified conditions are met. It may alter or delete data or entire files, cause a machine to halt, or do some other damage.
5) *Spyware* is a type of program installed to collect information about users, their systems or browsing habits, sending the data to a remote user. The collected information can be used by the attacker for blackmailing purposes or download and install other malicious programs from the web.
6) *Ransomware* is a type of malware that allows hackers to either block access to the hard drive or encrypt files at their will. It denies legitimate users access to their system and requires a payment, or ransom, to regain access. These attacks result in negative publicity and harm to one's reputation.
7) *Keylogger* refers to the action of recording the keys struck on a keyboard without the knowledge of the keyboard user.
8) *Back door / Trapdoor* refers to any method by which authorized and unauthorized users bypass normal security measures and root access on a computer system, network, or software application. The attackers can then remotely issue system commands and update malware.
9) *Zombie* is a computer connected to the Internet that has been compromised by a hacker via a computer virus, computer worm, or Trojan horse program which can be used to perform malicious tasks as per the remote instruction of the attacker.
10) *Bots* - A bot (short for "robot") is a program that can either run automatically or execute commands when they receive specific input. Common examples of bot programs are the crawler, chatroom bots, and malicious bots.

V. CYBER WARFARE

Cyber warfare is a cyberattack or series of attacks that target a country. It involves cyberattacks carried out by nation-state or international organization to damage another nation's digital networks through computer viruses or denial-of-service attacks. The intention of cyberwarfare is to "weaken, disrupt or destroy" another country.

Cyber warfare has the potential to wreak havoc on government and civilian infrastructure and disrupt critical systems, resulting in damage to the state and even loss of life.

VI. CYBER SECURITY

Cybersecurity refers to the protection the Internet, networked devices and data from cyber threats. It can be used by individuals and enterprises to protect against unauthorized access to networked devices. Cybersecurity protects data from theft and destruction.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XI Nov 2023- Available at www.ijraset.com

A. Types of Cyber Security

Types of Cyber Security include the following:

1) *Critical Infrastructure Security* - Critical infrastructure security involves the protection of critical systems, networks and assets whose continuous operation is essential to ensure the security of a given nation, its economy, and the safety and health of its people.
2) *Application Security* - Application security is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.
3) *Network Security* - Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
4) *Information Security* - Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. It ensures the protection and privacy of critical data such as customer account details, financial data or intellectual property.
5) *Cloud Security* - Cloud security refers to the technologies, policies, controls, and services that protect cloud data, applications, and infrastructure from threats.
6) *Internet of Things (IoT) Security* - IoT security is the technology segment focused on safeguarding connected devices and networks in the internet of things (IoT).

B. Protection from Cybercrimes

People should use cautious digital habits to protect themselves from Cybercrime. A few everyday practices will help you stay safe from cybercrimes. Ways to prevent cyber-crimes are explained below:

1) *Strong Passwords*: Use strong and unique passwords with 14-plus characters that includes a combination of alphabets, numbers and special symbols. Do not write them down. Maintain different password and username combinations for each of the accounts. Change passwords frequently. Examples of password combinations can make password more vulnerable to hacking:

- Using keyboard patterns for passwords. e.g. – wrtdghu
- Using very easy combinations. e.g. – sana1999, jan2000
- Using Default passwords. e.g. – Hello123, Madhu123
- Keeping the password the same as the username. e.g. – Madhu_Madhu

2) *Protect your identity online*: We must be cautious when giving our personal details such as name, address, phone number, and financial information on the Internet. Ensure that you use only safe websites to make online purchases and online transactions.
3) *Keep social media private*: Be sure that your social networking profiles (Facebook, Twitter, YouTube, etc.) are set to be private. Check your security settings. Exercise caution before you post information online. Anything put on the Internet once will be there forever.
4) *Use Safe Downloads*: Avoid downloading anything from an untrusted or unknown source. Make sure you are visiting a legitimate website.
5) *Use security software*: Make sure to update your computer with software updates especially your operating system. Security software includes firewall and antivirus software. Always install security software from trusted sources to protect your computer
6) *Avoid Public WiFi*: Avoid using Wi-Fi in public spaces as they are unsecured and unencrypted. Do not log in to your bank account in a public space or pay on an electronic commerce site.
7) *Secure your Devices*: Be sure to install the anti-virus software and to use a secure lock screen. Anti-virus software helps people to scan, detect, and remove threats before they cause serious problems. Update your antivirus software to get the best level of protection.
8) *Protect your storage data*: Protect your data by using encryption for your important diplomatic files related to finance and taxes.

9) *Safeguard against Phishing*: To safeguard against phishing attacks:

- *Critical thinking* — Do not open attachments in spam emails. Be cautious not to click on hyperlinks in spam emails or untrusted websites.
- *Analyzing email headers* — Email headers define how an email got to your address. Check whether the "Reply-to" and "Return-Path" parameters lead to the same domain as is specified in the email.
- *Hovering over the links* — Move your mouse over the link without clicking it in order to see where the link will actually take you. Apply critical thinking to decipher the URL.
- *Sandboxing* — People can test email content in a sandbox environment, logging activity from opening the attachment or clicking the links inside the email.

10) *Train Employees* - Continually train employees on cybersecurity policies and procedures and what to do in the event of security breaches.
11) *Keep an eye on your bank statements* - Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent.
12) *Parental Control* - Parents should monitor all the activities of their children online by monitoring their child's browser history and email accounts. Enable parental control in mobile apps, browsers, and at the router level so that kids will be able to access only the secured sites.
13) *Backup Data Regularly* - Backup information regularly to reduce the damage in case of a ransomware attack or data breach.
14) *Call the right person for help*: Try not to be nervous if you are a victim. When people suspect a cyber-crime or identity theft or a commercial scam, they should call the local police and complain on websites exclusively dedicated for cyber security.

C. *Combating Cyber Warfare*

There is no international law governing the use of cyber weapons but safety measures can be used to combat cyberwarfare.
Safety Measures to Combat Cyber Warfare
The following safety measures can be adopted to combat cyber warfare.

1) *Stay Protected* - Stay protected while connected. Use only Internet connection that is secure and password-protected. Avoid free Internet with no encryption. Do not use an unsecure public access point for sensitive activities that require passwords or credit cards.
2) *Conduct cyberwar games* - The best way to assess a nation's readiness for cyber warfare is to conduct a real-life exercise or simulation, also known as a cyberwar game. A cyberwar game can test how governments and private organizations respond to a cyberwarfare scenario, expose gaps in defenses, and improve cooperation between entities. It helps defenders learn how to act quickly to protect critical infrastructure and save lives. Cyberwar games can help cities, states, or countries enhance preparedness for cyber warfare by:
    - *Testing Different Situations* – Such as detecting attacks in early stages, or reducing risks after critical infrastructure has already been compromised.
    - *Testing unusual Scenarios* – Attacks are never conducted "by the book". Identify probable real threats and possible counter measures by conducting mock cyberattacks by Cyber Specialists.
    - *Collaboration* – Cyber warfare requires many individuals from different organizations and government units to collaborate. A cyber war game can bring together those people, who may not know each other, and help them decide how to work together in the event of a crisis.
    - *Policies Improvement* – Governments may establish cyber warfare policies and cyberwar games should be conducted to test the effectiveness of the policies and identify various ways to improve them.

D. *Cyber Security Tools*

Cybersecurity tools include the following:

1) *Network Security Monitoring Tools* - These tools are used to analyze network data and detect network-based threats.
   Examples: Argus, Nagios, Pof, Splunk, OSSEC.
2) *Encryption Tools* – They protect data by scrambling text so that it is unreadable to unauthorized users.
   Examples: Tor, KeePass, VeraCrypt, NordLocker, AxCrypt, TrueCrypt.

3) *Network Intrusion Detection Tools* – They monitor network and system traffic for unusual or suspicious activity and notifies the administrator if a potential threat is detected.
Examples: Snort, Security Onion, SolarWinds Security Event Manager, Kismet, Zeek.
4) *Packet Sniffers / Packet Analyzers* – They are used to intercept, log, and analyze network traffic and data.
Examples: Wireshark, Tcpdump, Windump.
5) *Firewall Tools* – A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
Examples: Tufin, AlgoSec, FireMon, RedSeal.
6) *Web Vulnerability Scanning Tools* – They scan web applications to identify security vulnerabilities including cross-site scripting, SQL injection, and path traversal.
Examples: Burp Suite, Nikto, Paros Proxy, SQLMap.
7) *Penetration Testing* – It simulates an attack on a computer system in order to evaluate the security of the system.
Examples: Metasploit, Kali Linux, Netsparker, Wireshark.
8) *Antivirus Software* – They are designed to find viruses and other harmful malware, including ransomware, spyware, adware, Trojans, and worms.
Examples: Norton 360, Norton AntiVirus, Kapersky Anti-Virus, McAfee Total Protection.

VII. DETECTING CYBERCRIMES

We can know that we are victims of cybercrimes if any of the following happens:
1) Unexpected call charges appear on your mobile phone bill.
2) You receive products you haven't ordered or paid for.
3) You receive unexpected and irrelevant post.

VIII. REPORTING CYBERCRIMES

Victims of cybercrimes can register a written complaint anytime to the cyber police or crime investigation department either offline or online. Victims can report to the cybercrime cell of any jurisdiction. Cyber criminals can be booked under Indian Penal Code 1860.

A. *National Cyber Crime Reporting Portal of India*

Through the National Crime Reporting Portal of India, the victims/ complainants can report cybercrime complaints online.
Examples of cybercrimes that can be reported to this portal include:
1) Online Child Pornography (CP),
2) Child Sexual Abuse Material (CSAM),
3) Sexually explicit content such as Rape/Gang Rape (CP/RGR) content and other cybercrimes such as mobile crimes, online and social media crimes, online financial frauds, ransomware, hacking, cryptocurrency crimes and online cyber trafficking.
4) The portal also provides an option of reporting an anonymous complaint about reporting online Child Pornography (CP) or sexually explicit content such as Rape/Gang Rape (RGR) content.

You can report a cybercrime at the online portal initiated by the Government of India.
https://cybercrime.gov.in/
https://staysafeonline.org/
https://digitalpolice.gov.in/
Cyber financial frauds reporting Number in India is 1930

IX. CYBER LAWS IN INDIA

In India, cyber laws are included in the Information Technology Act, 2000 ("IT Act"). The act came to effect on October 17, 2000. The act provides *legal permission for electronic commerce* and facilitates filing of electronic records with the Government.
A person who is proved guilty of data theft, virus transmission into a system, hacking, destroying data, or denying access to the network to an authorized person can be punished under Section 43 and 66 of the IT Act with *maximum imprisonment up to 3 years or a fine of rupees 5 lakh or both.*

X. CYBER SECURITY IN INDIA – PRESENT STATUS

In India, online frauds, data breaches and cyber scams are on a steep rise. Indians are affected by cybercrimes. Some of the cyberattacks that happened recently in India include:

1) In India, as per Government data, nearly 1.16 million cases of cyberattacks were reported in 2020. It amounts to an average of 3,137 cyber security issues reported every day of the year.

2) The average cost of a data breach in India in 2020 was $2 million, marking an increase of 9.4% since 2019 as per 'Cost of a Data Breach Report 2020' released by IBM.

3) At the start of COVID-19 pandemic, India has witnessed a 4000% increase in email phishing and a 400% spike in the number of policy violations.

4) It has been reported that 66% of organizations in India have suffered at least one data breach or cyberattack since shifting to a remote working model during the pandemic.

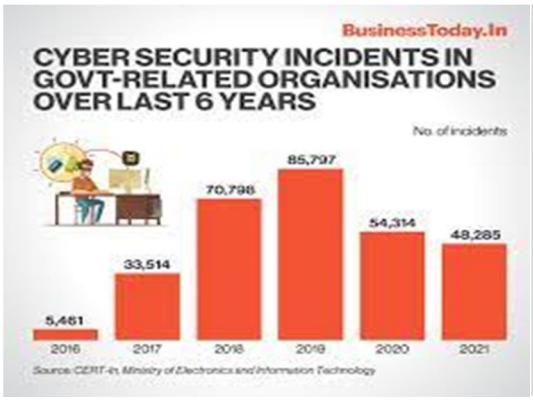


Fig. 4 Cyberattacks in Government Organizations

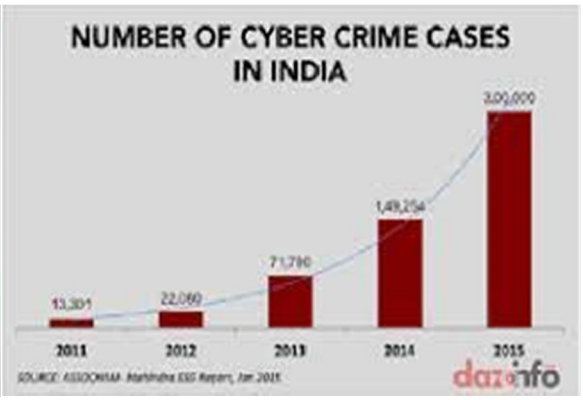


Fig. 5 Cybercrimes in India (2011-2015)

5) India is ranked third in the world among the top 20 countries being victimized by cybercrimes as per The Internet Crime Report by the FBI.

6) In January 2021, COVID-19 lab test results of thousands of Indian patients were leaked from government websites and the data was made publicly accessible on Google.

7) In February 2021, a database sharing forum went for sale of personally identifiable information (PII) of 500,000 Indian police personnel..

8) Upstox, India's second-largest stockbroker suffered a data breach in April 2021 that affected its 2.5 million customers. Over 56 million KYC details were leaked.

9) In November 2020, the data of 1.4 million Indian job seekers was leaked online after a cyberattack on the job portal IIMjobs.

XI. CONCLUSION

This paper explores various issues related to cybercrimes, cyberattacks, tools for cybercrimes, cyber warfare and cyber security. This paper also outlines various measures and steps that can be used by people, organizations, and governments to combat issues related to cybercrimes. The current scenario of cybercrimes in India are also presented. Cyberattacks are a never-ending problem. No permanent solution is currently available to prevent cybercrimes and cyberattacks. Effective Cyber security policies help individuals, business firms, and governments to reduce the loss and damage caused by various cyber security breaches. Creating awareness among the masses will immensely help alleviate problems caused by cyberattacks.

REFERENCES

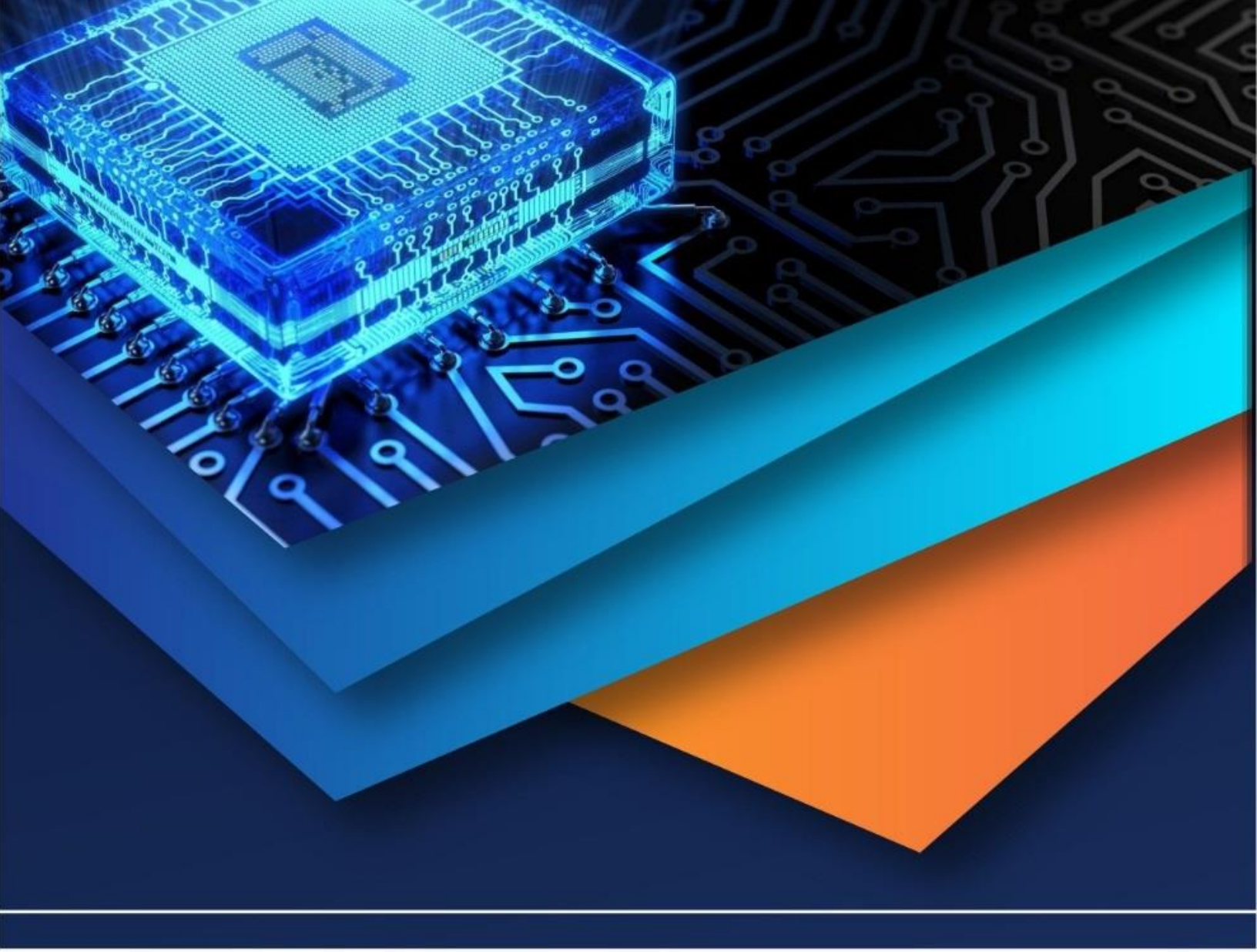
[1] J. Kaur, K.R. Ramkumar, The recent trends in cyber security: a review, J. King Saud University Computing. Information Science. 34 (8) 5766–5781, doi:10.1016/j.jksuci.2021.01.018, 2022.

[2] G. Srivastava, R.H. Jhaveri, S. Bhattacharya, S. Pandya, P.K.R. Rajeswari, Maddikunta, G. Yenduri, J.G. Hall, M. Alazab, T.R Gadekallu, in: XAI For Cybersecurity: State of the Art, Challenges, Open Issues and Future Directions, 1, pp. 1–33, 2022.

[3] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, K.K.R. Choo, Artificial intelligence in cyber security: research advances, challenges, and opportunities, Artif. Intell. Rev. 55 (2) 1029–1053, doi:10.1007/s10462-021-09976-0, 2022.

[4] V. Vouvoutsis, F. Casino, C. Patsakis, On the effectiveness of binary emulation in malware classification, J. Information Security Applications, 68 103258, doi:10.1016/j.jisa.2022.103258, 2022.

[5] H. Kavak, J.J. Padilla, D. Vernon-Bido, S.Y. Diallo, R. Gore, S. Shetty, Simulation for cybersecurity: state of the art and future directions, J. Cybersecurity, 1–13, doi:10.1093/cybsec/tyab005, 2021.
[6] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, S. Mahmood, Cyber security threats and vulnerabilities: a systematic mapping study, Arab. J. Sci. Eng., 45 (4) 3171–3189, doi:10.1007/s13369-019-04319-2, 2020.
[7] Europol. Internet Organised Crime Threat Assessment, https:// www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf, 2020.
[8] Backhaus S, Gross ML, Waismel-Manor I. et al. A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. Cyberpsychol Behav Soc Netw, 23:595–603, 2020.
[9] Connolly L, Wall SD. The rise of crypto-ransomware in a changing cybercrime landscape: taxonomising countermeasures. Computer Security, 87: 1–18, 2019.
[10] Valeriano B, Maness RC. Cyber War Versus Cyber Realities: Cyber Conflict in the International System, New York, Oxford University Press, 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY