Introduction to Cyber-Crime

Tambe Akshata Vasudeo[1], Shingate Vaishnavi Pramod[2]
[1,2] *Dept. Of Computer Science, S M Joshi College, Pune, Maharashtra, India.*

***Abstract*—Within the last decades modern society has become strongly dependent on the computer networks and ICT. However, that gave a rise to such a negative phenomenon as computer crime. Due to the rapid increase in usage of computers criminals gained a possibility to invade on more intimate spheres of life of individuals – their behaviour, life views, and habits. Trying to counter such an unlawful interference with private and family life of modern citizens competent authorities often fail to keep to the existing regulations which also leads to violations of the aforesaid right. This article gives a general view on the issue and provides with some offers regarding possible regulation. Within the last decades modern society has become strongly dependent on the computer networks and ICT. However, that gave a rise to such a negative phenomenon as computer crime. Due to the rapid increase in usage of computers criminals gained a possibility to invade on more intimate spheres of life of individuals – their behaviour, life views, and habits. Trying to counter such an unlawful interference with private and family life of modern citizens competent authorities often fail to keep to the existing regulations which also leads to violations of the aforesaid right. This article gives a general view on the issue and provides with some offers regarding possible regulation.**

***Index Terms*—Cybercrime, Privacy, Data Protection, Legal Frameworks, AI Fuzzing, IoT, GDPR, IT Act.**

I. INTRODUCTION

Cyber-crime is defined as any criminal activity which takes place on or over the computer or internet or any other information technology. cyber-crime is most common crime which plays any terrific role in modern world. Cyber criminals are not only causing looses to their identity to great extent. There are number of criminal activities done over the internet through skill full criminals. With increasing use of internet and computers in daily life. cyber-crime is also increasing internet provides convenience t the users but it has dark sides too. Cybercrimes may be of many kinds. It may also be stealing information, electronic money laundering, electronic terroism, salesfraud, investment fraud, illegal interception of communication, electronic funds transfer fraud, phishing, cyberwar, defamation or hacking personal website.

II.TYPES OF CYBERCRIMES

1. Cyber Bullying

It is also known as online or internet bullying. Cyberbullying happens when someone posts or shares harmful or mean content about someone else through the internet, socialmediaApps, videogames. Cyberbullying has top 10 forms such as Exclusion, Harassment, Outing, Cyberstalking, Fr-aping, FakProfiles, Dissing, Trickery, Trolling, Cat Fishing. This are the top 10 forms of cyber bullying.

2. Cyber Stalking

Stalking in general means behaviour of harassing or threatening other person. cyber stalking refers to stalking other person over the internet using information technology, in cyber stalking, internet, email, chats room etc., are used to stalk or harass an individual person. Stalking generally involves following a person, appearing at smokehouse or workplace, making harassing phone calls, emails etc. there are three ways in which Cyber Stalking is concluded-

- Staking by Email: -where the offender directly sends e-mail to the victim to threater someone or to harass someone. This is the most common type of Cyberstalking.
- Stalking through Internet: - In this the offender doesn't involve the private space of the victim but harasses her through the global medium publically. The offender through the internet medium posts the phone numbers and email address and put morphed pataes of victim in cyber space and threaten them.

- Stalking through computers: - In this, the offender takes the control of victim's computer as soon as computer starts operating. this form of stalking requires high degree of computer knowledge.

3. Data diddling

Data diddling also called false data entry. Data diddling is a type of cyber crime in which data is altered as it is entered into a computer system, most often by data clerk or a computer virus. For example: -A student could use data diddling to change their exam scores. They could use a computer program to alter the data in their school's records to make it look like they got a higher score on their exam than they actually did.

4. Phishing

Phishing is a type of cybercrimes where criminals send fake emails or messages pretending to be form a trusted organization like a bank, government office, or company.

Their aim is to steal personal detail, bank information, or passwords by tricking people into clicking on fake links. The message creates urgency like "Your Account will be blocked" or "You have won a lottery! Click the link now" People believe it and click the link. When they enter their details ,hackers steal them and misuse them.

5. Web jacking

Web jacking derives its name from "hijacking".

Web jacking is a cyber attack where attackers illegally gain control of legitimate website. They often, achieve this by exploring vulnerabilities in the website's owners. Or injecting malicious code. Bye compromising the website attackers can redirect users to fake websites designed to steal information, deface the website, or steal the website data. For example., in 2018, a popular online clothing store got hit by a web jacking attack. Hackers found a hole in the website's security and sneaked in malicious code. This made people who visited the site end up to a fake version that looked just like the real one. When customers typed in their credit card info and logins, the hackers stole it to buy stuff illegally or sell it on the dark web.

6.Identity Theft

Identity theft occurs when someone steals your personal information and uses it to commit fraud or other crimes. This sensitive information can include your social security number, credit card numbers, bank account information, etc. Identity thieves can use this information to open new accounts, make purchases, or even take out loans in your name. They may also use your information to commit other crimes, such as tax fraud or medical fraud.to protect yourself from identity theft, it's important to take steps to protect your personal information. This includes being careful about who you share your information with, using strong passwords, and monitoring your credit reports regularly.

7. Salami slicing attack

A salami slicing attack is a method of cybercrime that attackers or a hacker typically used to commit financial crimes. The salami slicing attack is considered as minor attack that can be repeated many times. It's a very small amount of money can be stolen from each customer's account in a particular bank. This type of attack is used for committing financial crimes, it is common and occurs within financial related organization. The salami slicing attack also used to gather information over a period of time to deduce on overall picture of organization.

8. Email bombing and spamming

Email bombing is an attack on your inbox That involves sending massive amounts of Message stolen your address. Also refers to flooding an email server with to manyemails in an attempt to overwhelm the email server and bring it down. Scamming practice in quickly.

9. Denial-of-Service attack

A Denial of service (DoS)attack is a type of cyber attack where an attacker deliberately floods a target system, network, or website with excessive traffic or request, causing it to become slow, unresponsive, or unavailable to legitimate users, Dos attacks typically involve a single source generating the malicious traffic. For Example., Imagine small business website hosted on a shared sever san attacker uses a tool to repeatedly send HTTP requests to the website's server, overwhelming its capacity to handle incoming traffic. As a result, the website becomes sluggish and eventually crashes, rendering it inaccessible to legitimate customers trying to access its services or make purchases. During the attack, the business loses

potential revenue and suffers damage to its reputation due to the inability of customers to access its website. This demonstrates how a DoS attack can disrupt the availability of the online services and impact businesses.

10. Distributed Denial-of-Service (DDoS) attack: -
A Distributed Denial of service (DDoS) attack is a type of cyber-attack were multiple compromised systems. Often infected with malware, are used to flood a target system, network, or website with a large volume of traffic. The overweening amount of incoming requests exceeds the targets capacity to handle them. Causing it to become slow, unresponsive, or completely inaccessible to legimate users.DDoS is the same ides but launched from many compromised machines at once, making it harder to block because the traffic is distributed. Attackers use botnets to flood bandwidth,CPU,or application resources. Mitigations included upstream scrubbing, CDNs, and traffic-anomaly detection.

III. LITERACTURE REVIEW

Cybercrime has become one of the most pressing challenges in the digital era, exploiting both technological vulnerabilities and human factors. Simultaneously, privacy concerns have intensified as personal, financial, and organizational data are increasingly stored, processed, and transmitted online. Scholars have explored cybercrime from multiple perspectives—technical, social, and regulatory—highlighting the interplay between criminal tactics and privacy breaches. Cybercrime is a multifaceted threat exploiting technology and human vulnerabilities. Literature shows the need for multi-layered defence strategies, combining technical safeguards, organizational policies, user education, and regulatory compliance. Future research should focus on evolving cyber threats, proactive mitigation measures, and the human factors influencing susceptibility.

IV. RESEARCH METHODOLOGY

This study is based entirely on **secondary data**, focusing on analyzing existing literature, academic research papers, industry reports, and case studies related to the use of Artificial Intelligence (AI), Robotics.

V. DATA COLLECTION SOURCES

The data for this research has been collected from a variety of **secondary sources**, including:

- Peer-reviewed journals and academic articles on Artificial Intelligence and Robotics
- Conference papers and white papers published by technology companies such as IBM, Google, and Microsoft, Google Scholar
- Industry reports from consulting firms like Google, DeepMind, Boston Dynamic
- Reliable online publications and case studies highlighting AI and ROBOTICS use in different fields.

These sources were carefully selected to ensure the data used is current, relevant, and credible.

VI. SCOPE OF THE STUDY

The scope of this study focuses on understanding the nature, techniques, impacts, and prevention of cybercrimes in the modern digital landscape. It examines cybercrimes from multiple perspectives, including technical, organizational, and legal aspects. Specifically, the study covers:

- Types of Cybercrimes
  - Financial crimes such as fraud, phishing, and salami slicing attacks.
  - Identity theft and data breaches affecting individuals and organizations.
  - Web-based attacks including web jacking, ransomware, and SQL injection.
  - Emerging threats targeting IoT devices, mobile platforms, and cryptocurrency systems.
- Cybercrime Techniques
  - Social engineering, phishing, malware, ransomware, and exploitation of software vulnerabilities.
  - Automation and AI-driven attacks, as well as insider threats.

Impacts of Cybercrimes

- Financial losses, privacy violations, reputational damage, and legal consequences for organizations and individuals.

- Prospects for responsible AI, safety protocols, and sustainable robotics.

VII. LIMITATIONS OF THE STUDY

- The research primarily focuses on technological evolution and societal impact, rather than in-depth technical implementation.
- Geographical and sector-specific applications may be highlighted selectively, based on available literature and case studies.

Future predictions are speculative and based on current technological satisfaction. This study focuses on the historical development, technological advancements, and societal impacts of cybercrimes, without providing detailed technical implementations. It primarily relies on existing literature, which may not capture the most recent developments or global variations. Discussions on ethical, social, and legal implications are conceptual and not based on empirical research. Additionally, predictions about future trends are speculative and may not fully reflect actual technological progress.

VIII. HYPOTHESIS

- Hypothesis: H1: Organizations with weak cybersecurity measures and low user awareness are more likely to experience cybercrime incidents, leading to financial losses, privacy breaches, and reputational damage.
- Explanation:
  This hypothesis focuses on the relationship between organizational preparedness and user behavior with the occurrence and impact of cybercrimes, providing a clear focus for data collection, analysis, and discussion in the study.

IX. DISCUSSION

The findings strongly support the study's hypothesis that Introduction To cybercrimes. Today the whole world is on the path of progress, but in this era of progress cyber crime has also increased a lot. Today we do many things through the internet. We do such things as online education, shopping, searching for jobs, communicating with each other through the internet. Cybercrimes are a bane to society. Cyber-crimes are a type of crime which include carrying out illegal activities while using technology, such as computers an internet. They have become extremely widespread and sophist in fact, it is a constantly evolving threat that can cause serious threats to individuals, governments, corporations and other financial organization. Cyber crimes can be of many types . one of the most wide spread type is a money heist which involve the robbery of money from big banks, wealthy individuals, financial organizations, and even the common man. Another type of cyber crime is hacking, which is the act of breaking into a computer system or network without authorization from the authorities.

X. RECOMMENDATION

The following recommendations are relevant to the world's research community, industry, government agencies and policy makers:

Cybercrime is a growing issue in India, involving malicious activities conducted using electronic devices or networks. It can be categorized into four main types: crimes against individuals, crimes against property, crimes against organizations, and crimes against society (Sarmah et al., 2017). Crimes against individuals involve activities like email spoofing, spamming, cyber defamation, and phishing, ISBN : 978-93-48796-55-4 Cyber Crime and Environmental Sustainability in India 100 where attackers manipulate email headers to deceive or harm victims. Spamming can clog email servers, reduce productivity, and lead to phishing scams, where attackers impersonate legitimate entities to trick users into divulging sensitive information. Cyber defamation harms individuals' reputations through digital platforms (Sarmah et al., 2017). Crimes against property involve cyber vandalism, software piracy, and unauthorized data modification or deletion, resulting in significant financial losses for victims. Intellectual property crimes, such as trademark infringement and copyright violations, also fall under this category. Crimes against organizations include hacking, unauthorized access to databases, and attacks aimed at disrupting business operations. Examples include Denial of Service (DoS) attacks, email bombing, and data diddling (Sarmah et al., 2017). Crimes against society, such as forgery and web jacking, violate individual privacy and create public mistrust towards digital platforms.

Understanding these nuances is crucial for safeguarding individuals, properties, and society (Sarmah et al., 2017)

XI. NATURE AND SCOPE

Crime is a socially correlated phenomenon. No matter how much we try. We cannot experience a society without cybercrimes. In actual sense, when we are not yet able to control the crime rate to the desirable minimum in the real world. How would it be possible to curb the same in the virtual world. Crimeless society is a myth and crime cannot be segregated from a society. Thus, the nature of the crime depends upon the nature of the society. Complexity of the society determines the complexity of the crime that envolves around it. To understand the crime in a society, it is essential and crucial to verify all the factors which influences and contribute to the crime. We have enact new laws and prepare preventive and defensive mechanism globally, only then we can able to protect out society from the evil called 'cyber-crime'. Therefore, the treat of cyber terrorism throws serious challenges to world and its agencies. The terrorist organizations using technology to spread hatred among people and using it to recuit militants and train them using teaching tools. they also launching websites which show them how to use weapons make bombs etc.

REFERENCES

[1] Furnell, S. 2002. Cyber Crime: Vandalizing the Information Society. London: Addison Wesley. (Open in a new window)Google Scholar

[2] Grabosky, P. 2001. "Virtual Criminality: Old Wine in New Bottles?" Social & Legal Studies 10: 243–249. doi:10.1177/a017405. View (Open in a new window)Web of Science ®(Open in a new window)Google Scholar

[3] Holt, T. J., and A. M. Bossler. 2016. Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Crime Sciences Series. New York: Routledge. (Open in a new window) Google Scholar

[4] Holt, T. J., A. M. Bossler, and K. C. Seigfried-Spellar. 2018. Cybercrime and Digital Forensics: An Introduction. 2nd ed. New York: Routledge. (Open in a new window) Google Scholar

[5] McGuire, M., and S. Dowling. 2013. "Cybercrime: A Review of the Evidence." Home Office Research Study. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248621/horr75-chap2.pdf(open in a new window) (Open in a new window)Google Scholar

[6] Tcherni, M., A. Davies, G. Lopes, and A. Lizotte. 2016. "The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?" Justice Quarterly 33: 890–911. doi:10.1080/07418825.2014.994658. View (Open in a new window)Web of Science ®(Open in a new window)Google Scholar

[7] Wall, D. S. 1998. "Catching Cybercriminals: Policing the Internet." International Review of Law, Computers & Technology 12: 201–218. doi:10.1080/13600869855397. View (Open in a new window)Google Scholar

[8] Wall, D. S. 2001. "Cybercrimes and the Internet." In Crime and the Internet, edited by D. S. Wall, 1–17. New York: Routledge. View (Open in a new window) Google Scholar