A STUDY ON THE ROLE OF ARTIFICIAL INTELLIGENCE IN PREVENTING CYBER CRIMES – INDIAN AND INTERNATIONAL PERSPECTIVE

Madhumitha P S, Alumna of School of Excellence in Law, The Tamil Nadu Dr. Ambedkar Law University

ABSTRACT

Technology has become rampant in all sectors. One of the most prominent technological tools to be used in almost all functional operations in current times is Artificial Intelligence. The term Artificial Intelligence (AI) is prominent in today's world driven by technology. In many ways, it is still an upcoming science in the light of problems present in today's dynamic environment. AI along with a closely related concept of cybercrimes are becoming common. Cybercrimes are being committed rampantly with the advent of technology and its use in committing them fails to control the consequences. AI and Cybersecurity are interdependent in contemporary cyber-security models. AI can greatly heighten the efficiency of any data security system by spotting potential threats coming to fruition and quashing cyber-attacks beyond human speeds.

This paper aims at highlighting the Concepts of Artificial Intelligence and Cyber Crimes and the Interface of AI in Preventing Cybercrimes in the Indian and International Perspective.

Keywords: Artificial Intelligence, Cyber, Crimes, Prevention, Cybersecurity, Indian, International.

I. INTRODUCTION

Technology has become an irreplaceable component in working sectors and of living. In today's technological world, the phrase Artificial Intelligence (AI) is widely used. In many ways, it is still a developing science in the current century. AI has managed to mark its significance in daily life from complex problem solving to content recommendation and virtual assistance. A form/kind of crime that is committed using the internet/technology and the recently developed AI is Cybercrime. Cybercrimes are gaining momentum and AI must be utilized to combat them alongside promoting Cybersecurity. This paper tries to examine the Role of AI in curbing Cybercrimes in the light of Indian and International Perspective.

II. CONCEPT OF ARTIFICIAL INTELLIGENCE

Meaning of Artificial Intelligence

Artificial Intelligence (AI) is the intelligence of machines/systems as opposed to human intelligence.

John McCarthy, a professor at Stanford, is credited with coining the phrase Artificial Intelligence, which he defined as "the science and engineering of creating intelligent computers."[1]

Objects of Artificial Intelligence

The primary objective of Artificial Intelligence is to make human life easier. The other range of objectives that can be achieved are solving complex problems, perceive dynamic environments, promote continuous learning, and find alternatives to accomplish decision making.

Categories of Artificial Intelligence

Artificial Intelligence can be categorized – [2]

[1] Professor Christopher Manning, *Artificial Intelligence Definitions*, 1 (2009), https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf

[2] TYPES OF AI WITH EXAMPLES, https://www.techtarget.com/searchenterpriseai/tip/4-main-types-of-AI-explained (last visited Dec. 9, 2024).

A. Based on Capability

1. General AI: To carry out normal human tasks in a computerized manner.

2. Narrow AI: To carry out specific goal-oriented AI tasks.

3. Super AI: To surpass human reasoning and intelligence to perform tasks.

B. Based on Functionality

1. Reactive Machines: To react appropriately based on current situations.

2. Theory of Mind: To understand human emotions and socially interact with them.

3. Self-Aware AI: To apply super intelligence machines with consciousness, emotions, and natural beliefs.

Process of Artificial Intelligence

AI is primarily used by reverse engineering human capacities and traits and applying them to machines. The process of AI involves the following steps – [3]

1. Data Input: Feeding input by way of speech, images, text, and context.

2. Data Processing: Interpreting data using rules and algorithms using the concepts of interpretations, prediction, and action.

3. Outcome: The final output or outcome can be of 2 kinds – success and failure.

4. Assessment: Determining the value of the outcome using the steps of analysis, discovery, and feedback.

5. Adjustment: Upon rectification of errors, the AI is ultimately updated.

[3] HOW DOES AI WORK?, https://www.geeksforgeeks.org/how-does-ai-work/ (last visited Dec. 9, 2024).

Challenges of Artificial Intelligence

AI stands at a point where its significance has become almost inevitable.

However, AI faces setbacks/challenges such as –

1. AI Algorithm Bias
2. Complex AI Integration
3. Possible Breach of Security
4. Unreliable Results.

III. CONCEPT OF CYBERCRIMES

Meaning of Cybercrimes

Cybercrime is a term that defines criminal activity using computer networks, computers, the Internet or even AI or when the tools become a target vice-versa.

Types of Cybercrimes

Cybercrimes can be divided into 3 categories –

A. Cybercrimes against Persons

   Individuals are the most prone targets and cybercrimes against them can include:

   1. Cyberstalking: Following a person's movement online using text messages, e-mail, social media, etc.
   2. Cyber Defamation: Posting defamatory content about a person online.

B. Cybercrimes against Property

   Property in the likes of computers, internet and digital technologies being targeted to gain unauthorized access or information and further misuse.

1. Intellectually Property (IP) Crimes: Infringement of IP such as patent infringement, software piracy and service mark violations.

2. Cyber Vandalism: Data Destruction or Damage caused by network outages or disruptions.

C. Cybercrimes against the Government

Targeting Government Property and Information can take place in the following types –

1. Cyber Terrorism: Endangering Government Websites, Portals, and Systems.

2. Possession of Unauthorized Information: Access to information that can be classified or sensitive to political or ideological objectives.

   The case *RVS Mani vs. Union of India* addressed cyberattacks by foreign entities on websites and databases of the Indian government with the aim of undermining national security and integrity. In order to effectively combat cyberterrorism, the court emphasized the significance of implementing strict measures and utilizing Section 66F of the IT Act.[4]

Enactment of Cyberlaws

To combat cybercrimes, various laws/legislations have been enacted in India such as:

A. Information Technology Act, 2000 (IT Act)

An Indian law that mainly regulates electronic transactions, e-commerce, and cybercrime. Various sections regulating cybercrimes are as follows-

[4] CYBERSECURITY LAWS AND REGULATIONS 2025, https://www.lexorbis.com/cybersecurity-laws-and-regulations-india-2025/ (last visited Dec. 10, 2024).

1. Section 65: Tampering with Computer Source Documents knowingly or intentionally.

2. Section 66: Computer Related Offences like Identity Theft, Cheating by Impersonation, etc.

3. Section 70: Unauthorized Access to Protected Systems

4. Section 72: Breach of Confidentiality and Privacy by accessing e-records, materials, or other documents without consent.

The Act also gives powers to Cyber Appellate Tribunals to hear appeals against the decisions of Adjudicating Officers punishing and sanctioning cybercrimes.

B. National Cyber Security Policy, 2013

A framework that defends India’s cyberspace and develops a safe cyber ecosystem by collaborating with businesses and stakeholders to spread knowledge about cybersecurity and implement cybersecurity solutions.

C. Digital Personal Data Protection Act, 2023

An Indian legislation that enables the processing of digital personal data in a manner that recognizes individual rights to protect personal data and process such data for lawful purpose.

D. Indian Penal Code, 1860/Bharatiya Nyaya Sanhita, 2024

The Indian Penal Code, 1860 was the official criminal code in the Republic of India inherited post-independence that covered all substantive aspects of criminal law and superficially including cyber law.

Various sections regulating cybercrimes are as follows –

1. Section 292: Sale of Obscene Material

2. Section 379: Theft

3. Section 420: Cheating and Dishonest Induction to Deliver Property

4. Section 499: Defamation (posting defamatory material online)

The IPC has been replaced by the Bharatiya Nyaya Sanhita, 2024 since 1st July 2024 and elaborates on cybercrimes under the following provisions – [5]

1. Section 18: Forgery (making false electronic record)

2. Section 75: Sexual Harrasment (showing pornography against the will of a woman)

3. Section 78: Stalking (monitoring the use of internet and online movements by a woman)

In *State of Tamil Nadu vs. Suhas Katti*[6], the victim's family friend, the accused, was her intended spouse; however, she wed another man, leading to a divorce. The accused convinced her once more after her divorce, and when she refused to marry him, he proceeded to harass her online. In the victim's name, the accused created a phony email account and posted offensive, offensive, and defamatory content about the victim. The accused was found guilty by the Additional Chief Metropolitan Magistrate in Egmore in accordance with Sections 67 of the IT Act and 469 and 509 of the Indian Penal Code, 1860.

To combat cybercrimes, various laws/legislations have been enacted in other countries such as–

A. United States of America: Computer Fraud and Abuse Act, 1986, Cybersecurity Information Sharing Act, 2015

B. Philippines: Cybercrime Prevention Act, 2012

C. United Kingdom: Computer Misuse Act, 2013.

[5] CYBERSECURITY LAWS AND REGULATIONS REPORT 2025 INDIA, https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india (last visited Dec. 10, 2024).

[6] State of Tamil Nadu v. Suhas Katti, CC No. 4680 of 2004.

IV. ROLE OF ARTIFICIAL INTELLIGENCE IN PREVENTING CYBER CRIMES – INDIAN AND INTERNATIONAL PERSPECTIVE

AI encompasses several strategies for protecting the integrity of networks, stored data, programmes, etc. against illegal tampering, illegal use, and hacker assault. Data breaches, identity theft, and other cyber-attacks are all prevented using the appropriate implementation of cybersecurity.

There are various AI Tools that can be used to combat cybercrimes such as –

1. Phishing Detection: Phishing is a common cybercrime in which attackers use messaging apps, social media, or emails to trick victims into disclosing important information. AI based solutions can help detect phishing attacks by analyzing the content of emails, links, and attachments. Algorithms using artificial intelligence (AI) can identify questionable patterns in email content or URL links and mark them for further investigation. To ascertain whether the email comes from a known phishing domain, AI may also look at its origin.

2. Threat Intelligence: Threat Intelligence collects and analyzes data from various sources to detect potential cyber threats. This technology can help organizations stay informed about emerging security risks and take proactive measures to avert attacks. Additionally, threat intelligence can be used to identify patterns and trends in cyber-attacks and aid organizations in determining where to direct their cybersecurity resources.

3. Security Information and Event Management: To effectively identify and mitigate cyber risks, Security Information and Event Management (SIEM), an AI-driven system, integrates security information management with security event management. Upon detecting a potential threat, SIEM gathers and analyzes log data from various systems and applications to issue real-time alerts. The AI algorithms utilized in SIEM enable security personnel to respond swiftly when patterns in log data indicate a cyber-attack.

AI's Role in the Prevention of Cybercrime can be understood in the Indian and International Perspective:

A. Indian Perspective

1. According to Karheek DN, Kumar MA and Kumar MRP (2012) in his article titled Reduction of Cyber Crimes by Effective Use of Article Intelligence:

   Security is the fundamental issue of cryptography. Using cutting-edge security techniques like the quantum channel can lessen cyberattacks.[7]

2. Every state in India has formed Cyber Crime Cells alongside Police Departments that are manned with qualified individuals who are experts in cybercrime investigation and are furnished with the newest technology and equipment to investigate cybercrimes.

3. To respond to cyber breaches and respond to government agencies, business partners, and international organizations, the Indian Government had created the Indian Computer Emergency Response Team (CERT-In or ICERT). It is an office under the purview of the Ministry of Electronics and Information Technology of the Government of India tasked to strengthen security-related defence of Indian Internet networks. It has been formed under Section 70B of the IT Act, 2000. It had launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) in 2017 as a citizen-centric service provider that dedicates to providing timely information about botnet and malware threats and suggesting remedial action for the same. CERT-In issued guidelines in April 2022 that called for reporting cyber incidents within 6 hours, maintenance of Information and Communication Technology (ICT) within Indian boundaries and obligations surrounding Virtual Private Networks (VPN) and Virtual Service Provider (VSP). In July 2024, CERT-In reported a computer outage relating to CrowdStrike Tools in MS Systems.[8]

[7] THE USE OF ARTIFICIAL INTELLIGENCE TO CURB CYBER CRIMES IN INDIA, https://www.legalserviceindia.com/legal/article-11906-the-use-of-artificial-intelligence-to-curb-cyber-crimes-in-india.html (last visited Dec. 11,2024)

[8] INDIAN COMPUTER EMERGENCY RESPONSE TEAM, https://en.wikipedia.org/wiki/Indian_Computer_Emergency_Response_Team (last visited Dec. 11,2024).

B. International Perspective

AI has also been used in other nations to effectively combat cybercrimes –

1. United States of America: The US Department of Homeland Security (DHS) uses the AI-powered National Cybersecurity Protection System (NCPS) to track and detect cyberthreats to federal networks alongside using machine learning methods to identify potential threats in real time and monitor network traffic.

2. Israel: Artificial intelligence is used by the Israeli Defence Forces (IDF) to detect and prevent cyberattacks on military networks. To identify potential threats instantly, the IDF uses machine learning algorithms to analyze network data. AI is also used by the IDF to develop prediction models that anticipate possible cyberthreats.

3. United Kingdom: AI is used by the UK's National Crime Agency (NCA) to detect and prevent child exploitation and internet fraud. In order to identify potential threats and suspects, the NCA uses machine learning algorithms to examine data from a variety of sources, such as social media and dark web forums.

V. AI AND CYBERSECURITY

With more data being stored and activities being conducted online, it has become easier for cybercriminals to gain illegal access and extract valuable information. The main goal of cybersecurity is to defend computers, networks, servers and online devices from various threats and malicious activities.

AI is promoted for cybersecurity using the following methods –

1. Assisted Intelligence: An emerging method of AI that allows organizations to perform tasks easier than what seemed impossible.

2. Augmented Intelligence: An emerging yet common method of AI that allows individuals and companies to improve existing measures.

AI is also made up of different subsets –

1. Machine Learning: Making use of various statistical tools that give systems the assurance to use data without being programmed to perform.

2. Neural Networks: Systems that lean and observe from data and produce results by summation of weights.

AI and Cybersecurity help improve the following activities –

1. Effectiveness of Controls

2. Information Technology (IT) Asset Inventory

3. Threat Exposure

AI and Cybersecurity help make advancements in the organization and protect the systems and data from all hacks and attacks.

VI. CONCLUSION

To conclude, Artificial Intelligence displays potential in reducing cybercrimes in India. Using AI's capacity to identify, prevent and respond to cybercrimes quickly and effectively is crucial given the growth in the trend. AI can be exploited to find patterns, trends, and abnormalities in the sphere of cyber-attacks. AI can be utilized even in law enforcement to track cybercriminals and detect potential threats. Hence, AI needs to be regulated in an elaborated manner and tapped effectively to combat the growing menace of cybercrimes.