Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
July-December 2023 4(2), 1358–1362

THE USE OF ARTIFICIAL INTELLIGENCE TO CONTROL CYBER CRIMES IN INDIA: AN OVERVIEW

Dr. Rang Nath Singh

[1] Principal, Rayat Bahra College of Law, Hoshiarpur, Punjab, India

DOI
10.29121/shodhkosh.v4.i2.2023.2418

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The term Artificial intelligence (AI) is prominent in the today's world of technology. In so many ways, it is still a developing science in light of the problems presented by the twenty-first century. AI use has been established in daily life. Since AI has such a significant influence on human existence now, it is difficult to comprehend a world without it. Simply define, artificial intelligence (AI) is the study of how people think, work, learn, and decide in every situation in life, whether it is connected to problem-solving, learning something new, thinking logically, or coming up with a solution, etc. Cybercrimes are becoming pretty common and frequently reported in the news. It is a global challenge, not simply one that affects one nation. AI is meaningless without strong security measures since it may be readily accessible by outsiders. Governments, banks, and global corporations now face a serious threat as a result of cyber security threats. Hackers use a lot of private and business data to their advantage.

Keywords: Artificial intelligence, Established, Cyber Crime, Accessible, Security

1. INTRODUCTION

Artificial intelligence (AI) has already been deployed in a multitude of applications to increase productivity, improve sales or enhance experiences. However, one crucial, though often overlooked AI application, is the focus of this report – enhancing protection against cyberattacks.

When used in conjunction with traditional methods, AI is a powerful tool for protecting against cybersecurity attacks. In the Internet Age, with hackers' ability to commit theft or cause harm remotely, shielding assets and operations from those who intend harm has become more difficult than ever. The numbers are staggering – Cisco alone reported that, in 2018, they blocked seven trillion threats on behalf of their customers.1 With such ever-increasing threats, organizations need help. Some organizations are turning to AI, not so much to completely solve their problems (yet), but rather to shore up their defences. As Martin Borrett, IBM distinguished engineer, chief technology officer and technical executive for IBM's European security business unit says, "Organizations are looking for automation, machine learning, AI to help make cybersecurity more manageable, more efficient, more effective and lower their risk.

Smart phones are now used by even illiterate individuals, and they are become a necessary element of modern life. If someone claims that today's people "live on the internet," they are not kidding. Internet use has gradually taken over as a vital element of daily life. Everyone uses AI in their daily lives without having the necessary awareness and comprehension.

Hackers have a fantastic opportunity to simply trick individuals at this moment. On occasion, hackers will mislead individuals with solid AI understanding. Despite adequate security measures, cyber-attacks are increasing fast. It may come in the form of malicious software, phishing, password assaults, drive-by downloads made possible via hyperlinks, virus attacks etc.

Cybercrime-

The newest and maybe most challenging issue facing the digital age is cybercrime. The phrase "cybercrime" has no definition under Indian law. In reality, even after being amended by the Information Technology (amendment) Act 2008, the Indian Cyber legislation, the Indian Criminal Code never refers to "cybercrime" at any time. Cybercrime refers to illegal actions using computers or the internet.

These are some examples of cybercrime: -

- Stealing and selling corporate data.
- Demanding payment to prevent an attack.
- Installing viruses on a targeted computer.
- Hacking into government or corporate computers.

Artificial Intelligence: -

Definitions Artificial intelligence (AI): -

Artificial intelligence (AI) is a collective term for the capabilities shown by learning systems that are perceived by humans as representing intelligence. Today, typical AI capabilities include speech, image and video recognition, autonomous objects, natural language processing, conversational agents, prescriptive modelling, augmented creativity, smart automation, advanced simulation, as well as complex analytics and predictions.

AI in cybersecurity: -

AI in cybersecurity a set of capabilities that allows organizations to detect, predict and respond to cyberthreats in real time using machine and deep learning.

Artificial intelligence is when machines, particularly computer systems, simulate human intelligence processes. Knowledge - based systems, natural language processing, speech recognition, and machine vision are some examples of specific AI applications. AI services and technologies are developing quickly. The 2012 Alex Net neural network marked the beginning of a new age of high-performance AI built on GPUs and massive data sets, which can be related to current advancements in AI tools and applications. The main advancement was the capacity to train machine learning on vast quantities of data simultaneously across several GPU.

Types of Cyber Crime in India: -

These are the main kinds of Cyber Crime: -

1-Financial frauds.
2-Hacking.
3-Cyber stalking and harassment.
4-Identity theft.
5-Intellectual property theft.

The effects of cybercrime: -

These are the effects of Cyber Crime: -

- Financial loss.
- Damage to reputation.
- Information loss.
- Legal repercussions.

TO overall, cybercrimes are a serious threat to people and businesses in India, thus it is important to take the necessary precautions to protect oneself from them. Strong passwords, updated software, and avoiding clicking on shady websites and emails are essential. Also, it's critical to notify law enforcement immediately of any cybercrimes:

2. LITERATURE REVIEW

Reduction of Cyber Crimes by Effective Use of Artificial Intelligence Techniques an article written by Kartheek D. N., Kumar M. A., Kumar M. R. P. (2012): - In this paper, cryptography techniques are highlighted. Security is the fundamental issue of cryptography. Cyberattacks can be reduced by implementing novel security methods like the quantum channel.
An article written by Govardhan. S. (2010) In his article, he focused more on the dynamic difficulties that cyber security faces. Hackers' intents nowadays are hostile, and in order to accomplish their goals, they are using unconventional methods, posing a serious danger to cyber security. He used the well-known example of Operation Aurora to illustrate his point.

Objective Of The research Paper: -
The main Objective behind writing this particular research paper is to assess how well AI techniques are performing at recognizing various cyber-attacks.
Methods Used to Curb Cybercrimes in India:

The IT Act of 2000, the National Cyber Security Policy of 2013, and the Cyber Crime Cells are some of the typical strategies utilized in India to combat cybercrime.

Some of the methods to curb cyber-crimes in India are following: -

I. In order to combat cybercrimes, each state in India has formed the Cyber Crime Cells, specialist forces. Along with the neighbourhood police department, these cells are in charge of looking into and prosecuting cybercrimes. The Cyber Crime Cells are manned with qualified individuals who are experts in cybercrime investigation.

II. To give legal validity to electronic transactions and to establish a legal framework for e-commerce, the IT Act of 2000 was established. Cybercrimes including hacking, identity theft, phishing, and cyber stalking are covered by the Act's provisions. The Act includes provisions for the creation of Cyber Appellate Tribunals to hear appeals against the decisions of Adjudicating Officers as well as sanctions and punishment for cybercrimes.

III. To establish a framework for the defence of India's cyberspace, the National Cyber Security Policy of 2013 was unveiled. The goal of the policy is to enhance the cyberspace regulatory framework and develop a safe cyber ecosystem.

IV. To respond swiftly to cyber-attacks and to coordinate responses with other government agencies, business partners, and international organizations, the Indian government has also developed the Indian Computer Emergency Response Team (CERT-In) in addition to these conventional techniques.

Overall, these conventional techniques have been successful in reducing cybercrimes in India; nevertheless, in order to keep up with the constantly developing nature of cyber threats, there is still a need for continuing investment in cybersecurity infrastructure and training for law enforcement agencies like;

The Information Technology Act, 2000 (IT Act):
To give legal validity to electronic transactions and to establish a legal framework for e-commerce, the IT Act of 2000 was established. Cybercrimes including hacking, identity theft, phishing, and cyber stalking are covered by the Act's provisions. The Act includes provisions for the creation of Cyber Appellate Tribunals to hear appeals against the decisions of Adjudicating Officers as well as sanctions and punishment for cybercrimes.
Unauthorized access to a computer system, computer network, or computer resource is a crime under Section 43 of the IT Act. Hacking is a criminal offence under Section 66, and transmitting offensive communications via communication services is a criminal offence under Section 66A. Identity theft is covered in Section 66B, and phishing is covered in Part 66C.

The 2013 National Cyber Security Strategy:
To establish a thorough framework for the defence of India's cyberspace, the National Cyber Security Policy of 2013 was unveiled. The goal of the policy is to enhance the cyberspace regulatory framework and develop a safe cyber ecosystem.

The strategy also aims to create collaborations with business, academia, and other stakeholder to spread knowledge about cybersecurity and create cutting-edge cybersecurity solutions. In conclusion, India has successfully reduced the number of cybercrimes through traditional measures such as the Cyber Crime Cells, the IT Act of 2000, the National Cyber Security Strategy of 2013, and the Indian Computer Emergency Response Team (CERT-In). Nonetheless, to stay up with the shifting nature of cybercrime, law enforcement agencies must continuously invest in cybersecurity infrastructure and training.

Following are some ways AI might reduce cybercrimes in India: -
1-Monitoring for cybersecurity:
2-Fraud detection:
3-Malware detection
4-Predictive analysis:
5-Support for investigations:

AI can help with cybercrime investigations by analysing massive amounts of data and finding patterns that might point to the origin of an attack. This can aid in the identification of suspects and the development of a case against them.
AI has the ability to significantly reduce cybercrimes in India. The nation's cybersecurity posture may be greatly improved by its capacity to analyse massive amounts of data, spot and pinpoint possible threats.

Some of the AI tools which can be used to Identify and curb crime in India are as following: -
Phishing detection: -
Phishing is a widespread cybercrime in which criminals deceive victims into divulging critical information by sending emails, using social media, or using messaging apps. By examining the content of emails, links, and attachments, AI-based systems can assist in the detection of phishing assaults. Artificial intelligence (AI) algorithms are able to spot suspicious trends in email content or URL links and flag them for additional examination. AI may also examine the email's origin to determine whether it originates from a known phishing domain.

Threat Intelligence: -
An AI-based service called threat intelligence gathers and examines data from numerous sources in order to identify possible cyber threats. This technology can assist businesses in keeping abreast of new security dangers and proactively preventing assaults. Threat intelligence may also be used to recognize patterns and trends in cyber-attacks.

Security Information and Event Management (SIEM): -
In order to identify and address cyber risks, security information and event management, or SIEM, an AI-based system, combines security information management with security event management. When a possible danger is identified, SIEM collects and analyses log data from numerous systems and apps to send out real-time warnings. Security workers can respond rapidly when trends in log data suggest a cyber-attacks thanks to the AI algorithms employed in SIEM.

Implementing AI-based solutions in India-
Lack of Standardization: -

AI-based solutions in India are not standardised, which may cause problems with interoperability. Integrating solutions from several suppliers can be challenging since different vendors utilise various frameworks. This may make it difficult to scale up solutions.

Regulatory Framework: -
India lacks a thorough regulatory framework for artificial intelligence. This may raise questions about how AI is used and regulated. To guarantee that AI is created and applied responsibly and ethically, a defined regulatory framework is required.

Bias in Data: -

Data bias is a major problem for AI, and it is also present in India. Many of the data sets employed in artificial intelligence-based solutions are skewed in favour of particular populations, such as urban regions or particular demographic groupings. Bias in data sets can be difficult to remove, and this might result in discriminating consequences for AI-based solutions.

Overall, putting AI-based solutions into practice in India is fraught with difficulties. Yet, India can overcome these difficulties and become a global leader in AI innovation with the correct investments in people, infrastructure, and legal frameworks.

3. CONCLUSION

To conclude we can say that Artificial intelligence (AI) offers a lot of potential for reducing cybercrime in India. Using AI's capacity to identify, prevent, and respond to cybercrimes quickly and effectively is crucial given the growth in their frequency. Deep learning, machine learning, and other AI-based tools may all be used to find patterns, abnormalities, and other signs of cyber-attacks. Moreover, AI can help law enforcement agencies locate and follow cybercriminals, analyse enormous amounts of information to find suspicious activity, and forecast and stop potential assaults.

India can remain ahead of the quickly changing cyber threat landscape and shield its citizens from the destructive consequences of cybercrime by incorporating Information into cybersecurity systems. Most cyberattacks can be stopped by practicing appropriate cyber ethics. In a nutshell, networked systems are utilised to conduct crucial business activities, making computer security a very wide field that has been growing increasingly critical.

4. RECOMMENDATION-

Some of the recommendations are as following: -

The Indian government may create AI-based training systems that mimic various cyberattacks, such as phishing, malware, and ransomware assaults, and offer instruction on how to avoid and respond to them.

Adopt AI-based cybersecurity measures: -

AI-based cybersecurity measures can be used to improve the efficacy of current cybersecurity measures. Systems for threat detection, intrusion detection, and prevention that are based on behaviour may learn from prior assaults and spot anomalies in real time.

The detection and prosecution of cybercriminals can be accomplished by establishing AI-based cybercrime investigative units. To analyse vast volumes of data and find fraudsters, these units can employ AI-based solutions. Systems powered by artificial intelligence (AI) may be used to find trends in criminal and create profiles of potential cybercriminals.

ACKNOWLEDGEMENTS

Authors are thankful to the healthcare practitioners working in GMC, Srinagar who helped directly or indirectly in the collection of data during the field work.

CONFLICT OF INTEREST

The authors declare no conflict of interest between them.

REFERENCES

Ankur Modi & Arunabh Chattopadhyay, Threat Intelligence in India: An Overview, 18 Int'l J. Comp. Applications 14 (2018).

2-Jyoti Prakash Singh, Arvind Kumar Yadav & Shalabh Kumar, Design and Implementation of SIEM System for Security Management in Indian Enterprises, 179 Int'l J. Comp. App. 9 (2018).

3-Muhammad Adnan Hashmi, Abubakr Muhammad, and Syed Muhammad Ali Abbas, "Artificial Intelligence Techniques for Cybersecurity: An Overview of Use Cases," IEEE Access, vol. 8, 2020, pp. 192267-192281.

4-S. Singh and S. Silakari, "A Survey of Cyber Attack Detection Systems", IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 5, 2009.

5-S. Dilek, H. and M. Aydın,"Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review", International Journal of Artificial Intelligence & Applications (IJAIA), vol. 6, no. 1, 2015.