The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

The Role of Artificial Intelligence in Cybercrime: A Comprehensive Analysis.

Abhilasha Soni

Table of Content

Conclusion

- Summary of key findings and insights.
- Closing remarks and suggestions for further study.

Abstract

The paper seeks to explain artificial intelligence, outline its fundamental elements, and provide examples of how it might be applied to the cybercrime system. Subsequently, identifying the different legal frameworks that guarantee the coexistence of artificial intelligence and human rights, as well as looking for domains in which AI might flourish in the fight against cybercrime and the realization of criminal justice.

This research paper also focuses on how advancements in digital technology have affected cybercrime globally also it deals with the use of AI in cybercrime cases with artificial intelligence playing a significant part in these changes. Since everyone has a different definition of what artificial intelligence (AI) is, the term itself is not properly defined. Most significantly, it is the ability of a non-human entity such as a computer to think and act like a human.

Artificial Intelligence (AI) has emerged as a powerful tool with transformative potential across various domains, including cybersecurity. However, alongside its positive applications, AI has also been increasingly exploited by cybercriminals to amplify the scale, sophistication, and efficiency of their illicit activities. This research paper provides a comprehensive analysis of the multifaceted role of AI in cybercrime, exploring its contributions to the evolution of attack techniques, its impact on defence strategies, and the ethical considerations it raises. Using artificial intelligence (AI) to solve cybercrime cases is a cutting-edge and successful approach as artificial intelligence (AI) has the capability to accurately forecast the specifics of future threats and give solutions but because it's a relatively new issue, it hasn't been fully studied and utilized. Thus, a thorough understanding of artificial intelligence's nature, adherence to fundamental principles, and application of these concepts to cybercrime will establish the foundation for the practical applications of law enforcement. An overview of artificial intelligence and its connection to cybercrime is provided in this paper also by examining

current trends, case studies, and future implications, this paper aims to deepen our understanding of the complex interplay between AI and cybercrime.

Keywords: cybercrime, artificial intelligence, advancement of technologies, benefits, threats, challenges, AI driven solutions.

Introduction

There are seldom new sorts of crime, but new technologies do bring new criminal opportunities. What sets cybercrime apart from other types of criminal activity? The usage of digital computers is obviously one difference, but technology by itself cannot account for each distinction that may exist between various domains of criminal conduct. To perpetrate fraud, traffic in child pornography and intellectual property, steal an identity, or invade someone's privacy, criminals don't need a computer.[1] Prior to the "cyber" prefix becoming widely used, all those activities existed. Cybercrime, particularly when it comes to the Internet, is a combination of new illegal activity and an expansion of already-existing criminal behaviour.

Cybercrime is the umbrella term for a broad range of illegal behaviours carried out via digital channels, such as identity theft, fraud, cyberbullying, hacking, and other online exploitation techniques.[2] These crimes seriously harm society, the economy, and people's mental health by taking advantage of flaws in digital systems. To address this expanding threat, it is imperative that we comprehend the nature of cybercrime and its effects on society.

The bulk of cybercrime consists of attacks on private, commercial, or government data. The set of data characteristics that characterise individuals and organisations on the Internet is known as the personal or corporate virtual body,[3] and this is where the attacks occur even though there is no physical body involved. To put it another way, in the digital age, our virtual identities play a crucial role in day-to-day existence. We are essentially a collection of codes and numbers stored in numerous computer systems that are controlled by businesses and governmental agencies. The prevalence of networked computers in our daily lives and the brittleness of seemingly indisputable concepts like personal identification are both highlighted by cyber.

---

[1] Jonathan Clough, Principles of Cybercrime 3–8 (2d ed. 2015).
[2] United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime 16–22 (2013).
[3] Jonathan Clough, *Principles of Cybercrime* 9–18 (2d ed. 2015).

Cybercrime has a wide-ranging and significant impact on society. Cybercrime causes companies and individuals to lose billions of dollars in revenue every year. The losses incurred are enormous.[4] The psychological effects on victims can be quite severe in addition to their money losses. If someone is the victim of cyberbullying, they may have suicidal thoughts and emotions of helplessness and violation, similar to identity theft victims.

Cybercrime also poses a significant threat to national security, as hackers target government agencies, critical infrastructure, and military systems. Such systems might be the target of a severe cyberattack that could compromise confidential information, interfere with vital services, or even result in bodily injury. Furthermore, faith in the digital economy and online platforms is weakened by cybercrime. The expansion of e-commerce and digital services may be hampered by people's reluctance to participate in online transactions or disclose personal information.[5] Cybercrime can also cause strain in international relations since it can lead to diplomatic tensions and wars when nations accuse one another of state-sponsored cyberattacks. Additionally, the spread of illegal operations like the dark web sales of firearms, drugs, and counterfeit products is another way that cybercrime affects society. In addition to fostering organised crime, these activities also exacerbate other social issues like addiction, violence, and human trafficking.

To sum up, cybercrime is a serious and developing menace to society that has far-reaching effects that go beyond monetary losses. Cybercriminals' increasingly complex strategies are developed as technology advances; thus, it is critical that people, organisations, and governments continue to be watchful and proactive in thwarting this threat.

Artificial intelligence (AI) is a leading technical advance that is reshaping almost every industry and drastically changing how we work, live, and interact with the world. Machines are now able to learn, reason, and make judgements thanks to this revolutionary technology that mimics human intellect. To grasp AI's benefits and problems, one must have a thorough understanding of its nature and how it affects society.

The creation of computer programmes that can carry out operations that normally call for human intelligence is referred to as artificial intelligence. Learners must be able to think, solve problems, perceive, and comprehend natural language, among other skills. Machine learning,

[4] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024 (2024).
[5] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024 (2024).

computer vision, natural language processing, robotics, and expert systems are just Several subfields that are included in the artificial intelligence category.

Artificial intelligence (AI) is radically changing society. Its effects are being felt in many different areas, and it is revolutionising our way of living, working, and interacting with one another. It has a significant transformational impact that presents society with both opportunities for progress and obstacles to overcome. AI boosts production and efficiency in all sectors. Robots with AI capabilities optimise manufacturing processes, increasing productivity and decreasing errors. AI is transforming healthcare through improved diagnosis and faster, more precise treatment. Moreover, chatbots and virtual assistants powered by AI are revolutionising customer service by offering fast, personalised assistance that improves consumer pleasure.

But there are worries about AI's ascent. A major problem is job displacement, especially in industries where regular work is essential. Retraining and upskilling the workforce is necessary to address this. Since AI presents important challenges regarding the gathering and use of personal data, privacy concerns have also come to light. Discrimination and bias are additional problems since AI systems may replicate the biases seen in the data they are trained on. Furthermore, as AI becomes more widely used, security vulnerabilities increase because hackers might use it to carry out increasingly complex and focused cyberattacks.

There are significant ethical ramifications for AI. As AI develops, concerns regarding its application in warfare, the moral treatment of AI-driven robots, and it's possible effects on human society surface.[6] As such, it is imperative to create strong rules, encourage the development of ethical AI, and make investments in workforce development and education. By doing this, society can guarantee that AI serves everyone and advances the development of a more just, prosperous, and technologically sophisticated future.

Main Body

The rise, use and development of AI in Cybercrime.

What is AI in cybersecurity?

Finding insights from data can be greatly aided by artificial intelligence, particularly machine learning. In the threat intelligence lifecycle, machine learning automates the steps of locating,

[6] United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime (2013).

contextualising, and ranking pertinent data.[7] This involves looking for posts on forums on the dark web that suggest a data leak and identifying questionable network activities. Security procedures may be improved, and new attacks can be promptly identified, prioritised, addressed, and remedied by security analysts with the help of machine learning in many cybersecurity fields.

This can aid in creating defence strategies and improving comprehension of earlier cyberattacks. Machine learning can be applied to a variety of cybersecurity sectors to improve security procedures and allow security analysts to promptly detect, rank, respond to, and neutralise emerging threats.[8] This can aid in creating defence strategies and improving comprehension of earlier intrusions. Traditional signature techniques differ from artificial intelligence (AI) in that they use machine learning (ML) algorithms to analyse large amounts of data, identify patterns and anomalies that may indicate the presence of a possible cyber-attack. Artificial intelligence is capable of rapid learning and developing defences, allowing it to identify and adapt to new and unknown threats.

How is AI used to tackle cybercrime?

Artificial intelligence plays an important role in cybersecurity, helping to identify and distinguish bad actors from good actors. Security systems using artificial intelligence react quickly and without delay, constantly scanning networks, devices and applications for possible threats and sending instant notifications to combat possible threats. AI has the ability to analyse past patterns and behaviour, allowing it to form a better understanding when encountering new or unknown information or study.[9] This allows the security team to make informed decisions based on the various options provided by the AI system, as it can come to accurate conclusions even with limited information.

Artificial Intelligence (AI) is emerging as a dependable alternative to existing security systems, which are becoming more and more slow and ineffectual in the face of increasingly complex cyberattacks. By using it, businesses may strengthen their cybersecurity posture and increase their defences against the constantly changing threat landscape.

The use of AI in detecting cybercrime.

[7] NITI Aayog, National Strategy for Artificial Intelligence (2018).
[8] Stuart Russell & Peter Norvig, Artificial Intelligence: A Modern Approach 693–721 (4th ed. Pearson 2021).
[9] Data Security Council of India, India Cyber Threat Report 2025 41–55 (2025).

In order to teach AI systems to detect malware and identify even the smallest behaviours of ransomware attacks, sophisticated algorithms are being deployed to execute pattern recognition tests on the systems before the threats penetrate. By using natural language processing to gather information about cyber dangers by searching through publications, news, and studies, artificial intelligence (AI) enables more accurate predictive intelligence. Given that fraudsters are always following patterns, this helps cybersecurity professionals better comprehend new abnormalities, cyberattacks, and preventive techniques.

AI-driven cybersecurity solutions provide up-to-date information on dangers that are specific to a given industry as well as those that are worldwide. In order to prioritise their defences against prospective assaults, this helps organisations make better informed decisions. As an illustration, a significant amount of internet traffic is generated by bots, which also pose a significant risk of account takeover and data theft. Nonetheless, businesses can distinguish between good and bad bots as well as human users with the aid of AI and machine learning, which can also help them better understand website traffic. Businesses are able to stay ahead of malicious bots and spot anomalous traffic patterns that can point to a security risk by examining behavioural trends.

- Cyber-crimes with Bharatiya Nyaya Sanhita (BNS), implications.

The following is the enumeration of the BNS provisions along with various cybercrimes that are attracted by respective sections and the punishment for the same. [10]

SECTIONS	PROVISION	PUNISHMENTS
294 of BNS	Although this section was drafted to deal with the sale of obscene material, it has evolved in the current digital era to be concerned with various cybercrimes. The publication and transmission of obscene material or sexually explicit act or exploit acts containing children etc which are in	Imprisonment – 2 years Fine – 5000 rupees. Subsequent Conviction Penalty: Imprisonment – 5 years Fine- 10,000 rupees

[10] Bharatiya Nyaya Sanhita, No. 45 of 2023, India Code (2023).

	electronic form is also governed by this section	
Section 77 of BNS	Under this law or provision taking or publishing a picture of a woman's intimate areas or actions without her consent is considered a cybercrime. This section only addresses the crime of "voyeurism," which also considers it illegal to witness a woman engage in such behaviour.	Imprisonment- 1 to 3 years And fine. Second or subsequent conviction or second time-offenders. Imprisonment- 3 to years 7 years. And is liable to fine.
Section 78 of BNS	This section defines and penalises “stalking”. Encompassing both online and offline stalking. Cyber-stalking occurs when a woman is being followed via email, the internet or electric communication or when she is contacted or interacted even though she doesn't want to.	For the first time offender Imprisonment – extending up to 3 years and is liable to fine. Second time offenders Imprisonment- extended up to 5 years and is also liable for fine.
Section 303 of BNS	If a mobile phone, the data from that mobile phone or computer hardware is stolen then these sections come into picture or play with penalties	Imprisonment- 3 years or fine or both.
Section 317(2) of BNS	This includes the following offenses punishable under Article 379. Any person who receives a stolen computer, mobile phone or information	Imprisonment – up to 3 years or fine or both

	related thereto will be punished under this section. It goes without saying that the thief must have the product. These provisions apply even if the information is in the possession of a third party who knows that it is someone else.	
Sections 319(2) and 318(4)	These laws have consequences because they target fraud. These two sections of the IPC clearly deal with various crimes, including password cracking with criminal intent, setting up fake websites and cyber-crimes. However, email phishing involves impersonating a person and asking for a password and is relevant only to Section 419 of the IPC.	319(2)- imprisonment up to 3 years or fine 318(4) - imprisonment up to 7 years or fine.
Sections 336 and 335 of BNS	Basically, what these sections contain Forgery, producing false records, fake electronic documents, records, and signatures are all punishable under this Section. This section deals with and punishes offences that occur in cyberspace, such as impersonating emails and creating fake papers	Imprisonment – extend up to 2 years or fine or with both.

Section 336(3) of BNS	Section 336(3) becomes relevant if the crimes of email spoofing and online forgeries are carried out with the intent to conduct other serious crimes, such as cheating.	Imprisonment – extend to 7 years and shall also be liable to fine.
Section 336(4) of BNS	If someone forges a document in person or uses electronic or digital means with the intent to defame a specific person, or if the forgery is carried out knowing that the victim will suffer from negative publicity.	Imprisonment- 3 years and shall also be liable to fine.

- Challenges and limitations in implementing AI driven defence solutions for cybercrime.

The use of artificial intelligence (AI) in the fight against cybercrime is becoming increasingly important. However, implementing artificial intelligence-supported defence systems has some problems and limitations. Organizations need to understand these issues to increase the effectiveness of their cybersecurity programs.

- Adversarial attack

Challenge: Defence measures powered by AI are seriously threatened by adversarial attacks. By altering input data, tricking AI algorithms, and resulting in misclassifications, cybercriminals might take advantage of weaknesses in AI models.

Limitation: AI models are still vulnerable to adversarial attacks even with major breakthroughs.[11] Effective detection and mitigation of adversarial manipulations necessitate constant monitoring, updating, and strengthening of AI models to defend against this attack.

- Data privacy and compliance

[11] Nat'l Inst. of Standards & Tech., Artificial Intelligence Risk Management Framework (AI RMF 1.0) 17–29 (2023).

challenge: In order for AI-driven defence systems to operate and train effectively, they need to have access to enormous volumes of data. However, this creates questions around the ethical use of personal data, data privacy, and regulatory compliance.

Limitation: Businesses have to tread carefully when it comes to data privacy and access. To address these concerns and preserve the effectiveness of AI-driven defence solutions, it is imperative to implement strong data anonymization techniques and ensure regulatory compliance.

- Skills gap

Challenge: One of the biggest barriers to the successful adoption of AI-driven defence solutions is the lack of cybersecurity specialists with AI experience. Specialised expertise and abilities are needed to develop, implement, and maintain cybersecurity systems driven by artificial intelligence.

Limitation: The successful acceptance and broad deployment of AI-driven defence solutions are impeded by the lack of qualified cybersecurity experts with AI knowledge.[12] To close the skills gap and create a skilled labour force, funding for training programmes and educational initiatives must be allocated.

- Over reliance on AI

Challenge: Relying too much on artificial intelligence (AI) for defence could lead to a false sense of security. Even if AI improves threat detection and response, human expertise and judgement cannot be replaced by AI; it is not a magic bullet.
Limitation: Companies need to balance automation powered by AI with human control. To assess complicated risks, formulate strategic options, and adjust to quickly changing cyberthreats, human intervention is essential.

- Threats of AI in cybercrime.

Even though artificial intelligence (AI) is largely acknowledged as a powerful weapon in the fight against cybercrime, it also poses a serious danger to these illegal operations. Cybercriminals are using AI more and more to create more complex and focused hacks as the

[12] Data Security Council of India, India Cyber Threat Report 2025 76–83 (2025).

technology develops. For organisations to properly improve their cybersecurity procedures, it is imperative that they comprehend these dangers.

- Automated and targeted attacks:

Threat: AI enables cybercriminals to automate and customize attacks on a large scale. With AI, attackers can develop malware that can adapt its behaviour to avoid detection, making it much more challenging for traditional cybersecurity systems to detect and mitigate.[13]

- Enhanced social engineering attacks

Threat: Artificial intelligence (AI) has the potential to produce incredibly lifelike chatbots, phishing emails, and social media profiles, which will increase the sophistication and difficulty of social engineering assaults. The success rate of social engineering attacks can be increased by using AI-driven chatbots that can have genuine conversations.

- Certain fake content

Threats: Artificial intelligence can create credible fake content, including images, audio, and video, that can be used to spread misinformation, cause deep conflict, or be used for many malicious purposes as an individual or organization.

- Password cracking

AI has the potential to greatly improve password-cracking methods. Patterns, vocabulary words, and personal data can all be more effectively analysed by AI-driven systems using complex algorithms to hack passwords.[14]

Case Laws

- Kalandi Charan Lenka vs state of Orissa (2016, Orissa High Court)

The victim here received certain obscene messages from an unknown number which was damaging the character of the victim. Additionally, emails were exchanged, and the defendant

[13] Data Security Council of India & Seqrite, India Cyber Threat Report 2025 33–45 (2025).
[14] Data Security Council of India & Seqrite, India Cyber Threat Report 2025 33–45 (2025).

created a fake Facebook account that altered the victim's photos. Therefore, the high Court found the accused prima facie guilty of cyberstalking under various sections of the Information Technology Act and Sections of BNS.[15]

- Gagan Harsh Sharma vs state of Maharashtra (2018, Bombay High Court)

One of the employers discovered that someone had compromised the computers and given the staff members access to private information. The employer also discovered that the software and data had been stolen. The employer provided the police with information, and they proceeded to register a case in accordance with the terms of the IT Act as well as Sections of the BNS. [16]

- Anil Kumar srivastava vs Addl director, MHFW (2005)

The petitioner electronically forged signature of AD and then later he filed a case making false proclamation or allegation about the same person. The court held that the petitioner was liable under section 465 as well as under section 471 of the Indian penal code as the petitioner also tried to use it as a genuine document. [17]

Suggestions

- Strategies to enhance AI in cybercrime.

By using artificial intelligence to create more complex and potent tools and tactics to support cybersecurity measures, cybercrime reduction through artificial intelligence can be achieved. Artificial intelligence driven technology can help us reduce the risks connected with cybercrimes and improve our defences against cyber-attacks.

Developing cybersecurity technologies with AI capabilities is one way to improve AI and lower cybercrimes. with the use of these tools, cyber risks can be found in real time by analysing enormous amounts of data to find patterns and anomalies. More efficiently than traditional, static security measures, AI-driven security systems can adapt to changing threats by continuously learning form fresh data.

To detect and stop cybercrimes before they happen, another tactic is to use AI for predictive analytics. AI is able to detect possible weaknesses and vulnerabilities in a system by evaluating

[15] Kalandi Charan Lenka v. State of Orissa, 2017 SCC OnLine Ori 133.

[16] Gagan Harsh Sharma v. State of Maharashtra, 2018 SCC Online Bom 1778

[17] Anil Kumar Srivastava v. Addl. Director, Ministry of Health & Family Welfare, 2005 Cri. L.J. 4314 (All.).

past data, giving organisation the ability to proactively correct these problems and stop assaults in the future.

AI can also be used to improve systems for access control and user authentication. organisations may improve security measures and make it more difficult for hackers to obtain unauthorised access to critical data and systems by utilising biometric data, behaviour analysis, and other AI-driven authentication processes.

Furthermore, AI can be quite helpful in obtaining threat intelligence. AI can detect new cyberthreats and give enterprises early warnings so they may take preventative action to safeguard their systems and data by evaluating enormous volumes of data from several sources.

To sum up, incorporating AI into cybersecurity can greatly improve defence mechanisms efficacy and efficiency, hence lessening the impact of cybercrimes. Through the deployment of AI- driven solutions, organisations may better safeguard their systems, data and users from unwanted activity by staying ahead of cyber threats.

- To promote and encourage the use of AI to reduce cybercrime.

Effective cybersecurity solutions in our digital age depend on promoting and encouraging the use of AI to decrease cybercrime. We can reduce the risks connected with criminal activity and improve our defence against cyber-attacks by utilising AI-driven technology.

Creating cybersecurity tools driven by AI is one such tactic. These tools enable the real-time identification of cyber threats by analysing large amounts of data to find patterns and anomalies. Compared to conventional, static security systems are able to continuously learn from fresh data and adapt to developing threats more efficiently.

Research into enhancing the interpretability of AI- driven cybersecurity solutions is also possible. Although deep learning models have shown remarkable results, they frequently function as “black boxes”, making it difficult to comprehend how they arrive at conclusions. By offering insights into the decision-making process, research on explainable AI techniques for cybersecurity can increase trust in AI-driven solutions and help cybersecurity professionals better comprehend and respond to these systems outputs. [18]

In conclusion, we can enhance the precision, scalability, and comprehensibility of AI-driven cybersecurity solutions by advocating and supporting their application. By doing this, we will

[18] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

be able to produce more potent weapons against cyberattacks and strengthen the defences around our digital infrastructure.

Conclusion

In conclusion, the intersection of artificial intelligence (AI) and cybercrime poses a serious and powerful threat to our digital environment. Cybercriminals can now turn to AI-driven technology to increase the intelligence and effectiveness of their attacks. The use of artificial intelligence (AI) to create malware, launch phishing campaigns, carry out malicious attacks, develop DDoS attacks, and create detailed investigations is related to the improper use of artificial intelligence in cybercrime such as disaster.

Nonetheless, there are plenty of chances to use AI to lower cybercrime. We can greatly improve our capacity to fend off cyberattacks by creating AI-powered cybersecurity tools, putting hybrid AI models into practice, and enhancing the interpretability, scalability, and resilience of AI-driven cybersecurity solutions. These developments will strengthen our digital defences by making it possible for us to identify and address attacks more skilfully.

As we continue to navigate the complex cybersecurity landscape, it is important to prioritize research and development measures that promote ethical and responsible behaviour. By supporting AI-driven cybersecurity innovation, we can improve our ability to protect systems, data, and users from attacks. Researchers, cybersecurity experts, policymakers, and stakeholders need to work together to create a safer and more secure digital ecosystem where AI is used for good rather than evil.