



AI AS A CATALYST IN THE EMERGENCE OF NEW CRIMES

** Dixit Vaishnavi Pradeep, ** Parashar Isha Ajay & *** Ms. Navya Premdarsh*

, **Students, * Assistant Professor, B.K. Birla College, (Empowered Autonomous Status), Kalyan.*

Abstract:

Artificial Intelligence (AI) has rapidly transformed modern society, improving efficiency across various sectors. However, its advancement has also contributed to the emergence of new forms of crime such as deepfake fraud, AI-based phishing, identity theft, and digital exploitation. This research examines AI as a catalyst in enabling sophisticated and large-scale criminal activities, with particular focus on its impact on women and children.

The study is based on secondary data collected from research papers, news reports, and credible institutional sources.

The research emphasizes the need for increased awareness, stronger cybersecurity measures, and responsible use of AI to ensure digital safety and protect society from emerging technological threats.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY-NC 4.0) which permits unrestricted use, distribution, and reproduction in any medium for non-commercial Use Provided the Original Author and Source Are Credited.

Introduction:

Artificial intelligence is used to complete tasks that require it to mimic human intelligence. It refers to a computer system that performs tasks like learning from data, recognising patterns, making decisions, and even generating text, images and voices.

AI did not appear suddenly. Its roots go back to the time when humans started wondering whether machines could think like humans. However, at that time, there was no technology capable of turning this idea into reality. AI existed only as a concept in human imagination.

During the 1940s, computers were used mainly for calculations and code-breaking. Seeing their ability to process information quickly, scientists began to believe that machines could be designed to perform tasks that required intelligence.

In 1950, A British mathematician Alan Turing asked an important question: “Can machines think?” He introduced the Turing Test, which proposed that if a machine could communicate so well that a human could not tell whether they were talking to a machine or another person, then the machine could be considered intelligent. This idea laid the foundation for Artificial Intelligence.

In 1956, the term “Artificial Intelligence” was officially introduced by John McCarthy at the Dartmouth Conference in the United States. Researchers at this conference believed that human intelligence could be fully simulated by machines. They were highly optimistic and thought that intelligent machines would be developed within a few decades. This marked the formal birth of AI as a scientific field.

In the beginning, Artificial Intelligence systems worked by following fixed rules given by humans. These systems could solve problems like calculations and games, but they could not handle real-life situations well. Later, AI development slowed down because computers were slow, costly, and the results did not meet

expectations. As technology improved, AI developed further with Machine Learning, where machines learned from data instead of depending on rules.

In recent years, AI has evolved into advanced forms such as Generative AI. This type of AI can create new content, including text, images, music, and videos. It works by learning from massive datasets and predicting the most suitable output. Although modern AI does not truly think or feel like humans, it can generate intelligent responses that closely resemble human behaviour.

In conclusion, Artificial Intelligence has grown from a simple idea into an important technology used in everyday life. Today, AI is applied in areas such as healthcare, education, business, law, and security. Although AI offers many benefits, its fast development also creates ethical and social concerns. Therefore, AI should be developed and used responsibly to ensure it benefits society.

AI has made many tasks easier and faster, its rapid growth has also created new challenges. One major concern is the rise of new forms of crime that use AI as a tool.

In the past, every major technological development has led to changes in criminal activities. AI does not create criminal intent, but it enhances the ability of criminals. It lowers the effort, skill, and time required to commit crimes. Earlier, many crimes required technical expertise or physical presence. With AI, even individuals with limited knowledge can commit complex crimes remotely. Criminals often adopt new technologies to carry out illegal acts in more efficient ways. AI acts as a catalyst in this process by allowing crimes to be automated and carried out on a large scale.

Crimes such as AI-based phishing, deepfake fraud, identity theft, and online manipulation are examples of how criminal methods are evolving with the help of AI.

As AI continues to grow and spread across society, it is important to understand how it contributes to the emergence of new types of crime. This research paper focuses on the role of artificial intelligence in enabling modern criminal activities.

Objective :

1. To create awareness about how Artificial Intelligence is misused for criminal activities and to explain its impact on society, so that individuals remain cautious and reduce their exposure to risks.
2. To prevent AI-based crimes by identifying effective cybersecurity measures and strategies that can minimize the chances of such crimes occurring.
3. To provide guidance to victims of AI-related fraud and threats by offering practical suggestions to manage situations and reduce further harm or damage.

Need for research :

The rapid advancement of Artificial Intelligence has led to the emergence of new and sophisticated crimes such as cyber fraud, identity theft, and deepfake misuse. Many individuals are unaware of how AI is exploited for criminal activities, which increases their risk of becoming victims.

This research is needed to understand the nature and impact of AI-enabled crimes, promote awareness and suggest preventive measures.



Research Methodology :

This research is based on secondary data collection. The study gathers information from already published sources to understand the role of Artificial Intelligence in the increasing rate of crimes.

Data has been collected from research papers and news articles.

Scope of the Study :

This study examines the emerging misuse of Artificial Intelligence in crimes that disproportionately affect women and children. It explores technology-driven threats such as manipulated images and videos, online exploitation, harassment, identity misuse, and digitally facilitated abuse. While particular attention is given to the vulnerabilities faced by women and minors, the study also considers relevant instances from the broader landscape of AI-enabled crimes to provide a more comprehensive understanding of how such technologies are reshaping criminal behaviour across different contexts.

Limitations of the Study :

This study relies on secondary data from published research papers, reports, and credible sources. Primary data collection was not conducted.

There was limited access to official government records and case-specific data related to AI-based crimes.

Many AI-enabled crimes remain unreported in official statistics. This affects the accuracy of the available data. There is significant underreporting due to fear, social stigma, and lack of awareness, especially in cases involving women and children.

Additionally, there is a lack of gender-based data specifically identifying AI-related crimes against women and children, which limits detailed analysis.

Review of Literature :

Researches:

Kiran et al. (2021), in their study titled Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI, examined how AI technologies are misused for crimes such as phishing and identity theft. The study highlighted that while AI improves efficiency, it also enables more sophisticated criminal activities and creates regulatory challenges.

Sai and Wang (2022), in their study titled Criminal Regulatory Approaches to Deepfake-Related Offenses, examined the use of deepfake technology in fraud. The study highlighted that AI-generated content is increasingly used for impersonation, posing challenges to existing legal systems.

Lin (2022), in his study titled Examining the Role of Deepfake Technology in Organized Fraud, analysed the use of AI in organized financial crimes. The research found that deepfake technology increases the scale and complexity of fraud, making detection difficult.

Marchal et al. (2024), in their study titled Generative AI Misuse: A Taxonomy of Tactics and Insights from Real-World Data, analysed real-world misuse of generative AI. The research found that AI tools have lowered the barrier for committing cyber and financial crimes.



Zhang et al. (2023), in their study titled AI-Based Identity Fraud Detection, examined AI-driven identity fraud. The study highlighted that advancements in AI have increased the sophistication of identity-related crimes News articles

Case: Hong Kong Deepfake Scam – (source CNN)

A Hong Kong finance worker was tricked into sending about \$25 million after fraudsters used deepfake technology to impersonate the company's UK-based CFO and other colleagues in a fake video call. Police said the scam was discovered only after the employee checked with head office, and several arrests have been made in related deepfake fraud cases.

Assam Man Arrested for AI-Generated Explicit Videos (2025) – (source NDTV)

In Tinsukia district, Assam, police arrested a man for allegedly creating AI-generated pornographic videos using morphed photographs of a woman.

According to police, he used her images and digital tools to fabricate explicit videos and circulated them on social media. The accused also reportedly earned money by distributing these manipulated videos.

The case highlights how AI image-generation and deepfake tools can be used for revenge harassment, extortion, and online exploitation.

Bengaluru Woman Loses ₹3.75 Crore to Deepfake Video Scam – (source NDTV)

On 25th February 2025, a 57-year-old woman in CV Raman Nagar, Bengaluru lost approximately ₹3.75 crore after falling for a deepfake video of spiritual leader Sadhguru promoting a stock trading platform. The AI-generated video appeared authentic and convinced the victim to invest large sums, after which she was added to a WhatsApp group and persuaded to transfer funds over time. Police stated she was unaware that the video had been digitally fabricated using deepfake technology before discovering the fraud and filing a complaint.

Influencer Loses ₹1.1 Lakh After AI-Powered Fake KYC Scam – (source NDTV)

In 2025, an Indian social media influencer publicly revealed how she lost ₹1.1 lakh after clicking a convincingly fake KYC link that mimicked her bank's official interface. The phishing page employed AI-generated text and bot-automated responses to lull victims into a false sense of security, prompting them to enter sensitive credentials, OTPs, and authorization codes.

Once the attacker harvested her data, unauthorized transactions drained funds from linked accounts. Banking regulators later cited this as a growing trend where AI-assisted phishing and automated scripts make scams far harder to detect visually.

Columbia suspends student who created AI tool that helps people cheat in coding interviews – (Source: Business Insider)

Chungin "Roy" Lee, a student at Columbia University, was suspended for a year after creating an AI tool called Interview Coder that helps people cheat during technical coding interviews by providing hidden real-time answers. The university said the suspension was for posting disciplinary materials online, not simply for building the tool. Lee had shared social media posts about a disciplinary hearing and faces suspension from the school, as documented in the university's conduct letter



AI-Generated Fake Child Abuse Images Lead to Arrest – (Source: BBC)

Hugh Nelson, 27, has admitted to 11 offences after using AI technology to create and distribute indecent images of children. Appearing at Bolton Crown Court, he pleaded guilty to charges including attempting to incite a boy under 16 to engage in sexual activity, making and distributing indecent images, possessing prohibited material, and publishing obscene content. Police described the case as “particularly unique and deeply horrifying” because Nelson used computer software to transform normal photographs of real children into indecent “pseudo-photographs.” He is due to be sentenced on 25 September.

Dozens arrested in global hit against AI-generated child abuse – (Source BBC News)

At least 25 arrests have been made during a worldwide operation against child abuse images generated by artificial intelligence (AI), the European Union’s law enforcement organisation Europol has said. The suspects were part of a criminal group whose members engaged in distributing fully AI-generated images of minors, according to the agency.

Illinois student arrested after child porn allegedly found in dorm – (Source NewsNation)

According to the DeKalb County Sheriff’s Office, 19-year-old Michael Erickson, a current student at Northern Illinois University, has been charged with 21 felonies, including production of child pornography, dissemination of child pornography and possession of child pornography.

The Grok case is just the tip of the iceberg – (Source University of Oxford)

Grok, Elon Musk’s AI chatbot, is under criticism for generating sexualised images of women and minors without consent. Users can upload photos, alter them, and share the results publicly on X.

Although warnings were issued, the issue isn’t new—the system has reportedly had weak safeguards since launch. The recent backlash has only highlighted long-standing concerns about misuse and lack of control.

Woman felt ‘dehumanised’ after Musk’s Grok AI used to digitally remove her clothes – (Source BBC)

A woman has told the BBC she felt “dehumanised and reduced into a sexual stereotype” after Elon Musk’s AI Grok was used to digitally remove her clothing. The BBC has seen several examples on the social media platform X of people asking the chatbot to undress women to make them appear in bikinis without their consent, as well as putting them in sexual situations.

Literature Analysis :

The reviewed studies highlight the misuse of artificial intelligence in crimes such as phishing, identity theft, deepfake fraud, and financial crimes. However, most of these researches focus on specific categories of AI-enabled crimes, particularly deepfake and financial fraud, which limits a broader understanding of AI as a catalyst for diverse and emerging criminal activities.

While existing studies offer strong conceptual and regulatory insights, limited attention has been given to newly emerging forms of AI-driven crimes and their specific impact on women and children. These vulnerable groups face unique risks such as online exploitation, deepfake abuse, grooming, cyber harassment, and digital manipulation, which remain underexplored in current research.



Currently, there is no single, consolidated official database provided by the government specifically for AI-based crimes. Therefore, the statistics included in this study have been compiled and analysed from multiple credible and recognized sources.

These combined figures help in understanding the growing trend, patterns, and impact of AI-related crimes across different regions. By reviewing existing literature and reported cases, this analysis aims to present a clear overview of how Artificial Intelligence is emerging not only as a technological advancement but also as a tool that can be misused for criminal activities.

Deepfake fraud increased by 1,740% (2022–2023) – World Economic Forum

The World Economic Forum reports a 1,740% surge in deepfake-enabled fraud attempts in North America between 2022 and 2023. This sharp rise reflects the rapid adoption of generative AI in financial and identity-related crimes, particularly in bypassing authentication systems and enabling large-scale fraud.

Over 105,000 deepfake-related cases in the U.S. – The Wall Street Journal

The Wall Street Journal notes that deepfake-related incidents exceeded 105,000 reported cases in the United States. These cases included identity theft, impersonation, and financial scams, highlighting the growing scale and sophistication of AI-driven cybercrime.

The above figures are based on secondary data, therefore, this section examines statistical findings reported by recognized institutions and publications such as the World Economic Forum and The Wall Street Journal.

Conclusion :

Artificial Intelligence has transformed from a theoretical concept into one of the most powerful technologies of the modern era. From the ideas of Alan Turing to the formal recognition of AI as a scientific discipline at the Dartmouth Conference, its journey reflects continuous innovation and rapid technological growth. Today, AI supports progress in healthcare, education, business, and governance. However, as this research highlights, the same technology that drives development can also be misused for harmful purposes.

The study demonstrates that AI has not created criminal intent, but it has significantly enhanced the scale, speed, and sophistication of criminal activities. Statistical data compiled from recognized institutions clearly indicate a sharp rise in AI-enabled fraud and impersonation cases worldwide. Although there is no consolidated official government database exclusively dedicated to AI-based crimes, the combined analysis of credible secondary sources reveals an alarming upward trend.

This research further emphasizes that limited awareness, lack of digital literacy, and inadequate cybersecurity practices makes any individual an easy target. At the same time, law enforcement agencies face growing challenges in detection, attribution, and prosecution due to the evolving and borderless nature of AI-driven crimes.

Therefore, the findings underline the urgent need for a multi-dimensional response. Awareness programs must educate individuals about emerging AI-related risks. Preventive strategies, including stronger cybersecurity systems and verification mechanisms, must be strengthened. Most importantly, technological advancement must be accompanied by ethical responsibility.

In conclusion, Artificial Intelligence is neither inherently good nor bad, it is a tool whose impact depends on how it is used. While AI continues to shape the future of society, it is essential to ensure that its development aligns with principles of safety, accountability, and social welfare. Only through collective efforts involving policymakers, researchers, law enforcement, organizations, and citizens can AI be guided toward innovation that benefits humanity rather than enabling harm.

Suggestions :

Suggestions for Awareness :

1. Awareness Campaigns in Rural and Sub-Urban Areas

Conduct local workshops and community drives to educate people about AI scams. Face-to-face awareness builds trust and understanding.

2. Communicate in Simple and Local Language

Avoid technical terms and use regional languages. Simple communication helps people understand risks clearly.

3. Promote Cybercrime Helpline Awareness

Publicize helpline numbers and reporting portals widely. Quick reporting can reduce financial loss.

4. Awareness Ad Campaigns on TV and Social Media

Use short, realistic ads to show how AI scams happen. Repeated messaging increases caution.

5. Use Real Victim Stories (With Consent)

Share real cases to make the risk feel real. Personal stories create stronger impact and awareness

Suggestions for Prevention :

1. Strengthen Digital Literacy

Teach people how to identify fake calls, messages, and AI-generated content. Basic digital knowledge reduces vulnerability.

2. Encourage Verification Before Action

Always verify suspicious calls or video messages before sending money or sharing details. A simple call-back can prevent major fraud.

3. Stronger Data Privacy Practices

Avoid sharing personal information, OTPs, or financial details online. Limiting data exposure reduces misuse by scammers.

4. Use Strong Security Measures

Enable two-factor authentication (2FA) and use strong, unique passwords for accounts. Extra security layers make hacking more difficult.

5. Immediate Reporting and Awareness Sharing: Report suspicious activities immediately to authorities and inform family or friends. Quick action can prevent others from becoming victims.

Suggestions for Victims:



1. **Report Immediately:** Contact the national cybercrime helpline or online portal as soon as possible. Quick reporting increases the chances of recovery.
2. **Inform Your Bank Quickly:** If money is involved, immediately notify your bank to freeze transactions. Early action can stop further loss.
3. **Preserve Evidence:** Save call records, screenshots, transaction details, and messages. This evidence helps authorities investigate the case.
4. **Seek Emotional Support:** Victims should not feel ashamed or blame themselves. Talking to family or trusted people can reduce stress and anxiety.
5. **Spread Awareness After Recovery:** Share your experience (with comfort and consent) to warn others. Your story can prevent someone else from becoming a victim.

References:

1. Kumar, M., Kalanjali, R., Lava Kumar, S., Nithish Kumar, E., Kiran Kumar, G. and Divakar, D. (2024). *Artificial Intelligence Crime: An Overview Of Malicious Use And Abuse Of AI*. [online] 10(2). Available at: https://ijariie.com/AdminUploadPdf/ARTIFICIAL_INTELLIGENCE_CRIME_AN_OVERVIEW_OF_MALICIOUS_USE_AND_ABUSE_OF_AI_ijariie23586.pdf
2. [Accessed 2 Mar. 2026].
3. Sai, S., & Wang, Z. (2024). *Criminal regulatory approaches to deepfake-related offenses: Focusing on the crime of fraud*. *International Journal of Asian Social Science Research*. <https://doi.org/10.70267/ijassr.260301.2031> Zeus Press Journals
4. Lin, L.S.F. (2025). *Examining the Role of Deepfake Technology in Organized Fraud: Legal, Security, and Governance Challenges*. *Frontiers in Law*, [online] 4, pp.6–17. Doi : <https://doi.org/10.6000/2817-2302.2025.04.02>.
5. Marchal, N., Xu, R., Elasmr, R., Gabriel, I., Goldberg, B., & Isaac, W. (2024). *Generative AI misuse: A taxonomy of tactics and insights from real-world data*. *arXiv*. <https://arxiv.org/abs/2406.13843> arXiv
6. Zhang, C.J., Gill, A.Q., Liu, B. and Anwar, M.J. (2025). *AI-based Identity Fraud Detection: A Systematic Review*. [online] *arXiv.org*. Available at: <https://arxiv.org/abs/2501.09239>.
7. Altchek, A. (2025). *Columbia suspends student behind interview cheat AI tool*. [online] *Business Insider*. Available at: https://www.businessinsider.com/columbia-suspends-student-ai-interview-coder-cheat-tool-chungin-lee-2025-3?utm_source=chatgpt.com.
8. Burgess, J. (2025). *AI-generated child abuse global hit leads to dozens of arrests*. *BBC*. [online] 28 Feb. Available at: <https://www.bbc.com/news/articles/czxnnzz558eo>.

Cite This Article: Dixit V.P. & Parashar I.A. (2026). *AI As A Catalyst in the Emergence of New Crimes*. In *Educreator Research Journal: Vol. XIII (Issue I)*, pp. 166–173. Doi: <https://doi.org/10.5281/zenodo.20205225>