IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657
Volume 10, Issue 4, Dec 2022

ARTIFICIAL INTELLIGENCE CRIME' AN OVERVIEW OF MALICIOUS USE AND ABUSE OF AI

[1] Kamireddy Uday Kiran, [2] Dr Ravindar Reddy Thokala,[3] Himabindu Chinni, [4] Madupu Bobby

[1,2,3] Assistant Professors,Department of Computer Science and Engineering, Brilliant Grammar School Educational Society's Group Of Institutions, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

[4]student,Department of Computer Science and Engineering, Brilliant Grammar School Educational Society's Group Of Institutions, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

ABSTRACT

The fast development of AI technology has resulted in several positive outcomes, but it has also presented new threats and difficulties linked to its misuse and bad intent. An extensive survey of AI-related crimes is presented in this research, which delves into the whole range of evildoings that take use of AI systems for immoral and unlawful ends. Automated phishing, deepfake generation, and data breaches are some of the cyberattack vectors discussed. Furthermore, the project explores the negative applications of AI in monitoring and invasions of privacy, drawing attention to the ways in which these technologies might be used to violate civil liberties and personal freedoms. This paper seeks to illuminate the many types of AI misuse and provide suggestions for reducing related risks by conducting a thorough examination of case studies, regulatory loopholes, and upcoming threats. The goal of this project is to raise awareness of the fact that AI technology may be used for both good and evil, and to help create regulations and policies that will help stop crimes using AI.

I. INTRODUCTION

With its superior data processing, automation, and decision-making capabilities, artificial intelligence (AI) has sparked a revolution in a wide range of businesses. While AI has the potential to revolutionise several areas, it also poses

fresh avenues for dishonest conduct. There have been more reports of AI systems being abused and misused as they have become more advanced, which

ISSN 2347–3657
Volume 10, Issue 4, Dec 2022

has led to serious worries about their ethical and cybersecurity consequences. The overarching goal of this project is to provide a comprehensive review of crimes using artificial intelligence, with a particular emphasis on the criminal exploitation of AI technology. Cyberattacks, privacy issues, and misleading content generation are some of the ways artificial intelligence (AI) has been misused. The goal of this project is to bring attention to the dangers of AI and suggest ways to lessen them by looking at actual instances and finding critical weaknesses. The objective is to encourage the creation of appropriate regulations and protections to fight AI-related crimes and to promote a greater knowledge of the dual-use nature of AI technology.

II.EXISTING SYSTEMS

The present methods for dealing with crimes connected to AI often use conventional ethical and cybersecurity frameworks, which could not adequately tackle the specific difficulties presented by AI systems. For example, typical security measures like intrusion detection systems and firewalls are used by a lot of current systems, but they may not be able to identify complex assaults powered by AI. Because they can create very convincing and tailored material, automated phishing assaults driven by AI may bypass conventional email filters and detection systems [1]. Similarly, current media verification systems face substantial problems from deepfake technologies, which generate realistic but faked media material [2]. There may be loopholes in the present privacy legislation that allow for the use of AI for data collecting and spying [3]. Because of these restrictions, we need better, AI-specific solutions to stop bad actors from using AI.

III.PROPOSED SYSTEM

By using modern security mechanisms and ethical norms tailored to AI, the suggested system offers a comprehensive strategy to tackle crimes involving AI. This strategy entails creating anomaly detection systems powered by AI that can spot suspicious patterns and behaviours. As an example, distinguishing features of AI-generated material, such deepfakes or phishing attempts, may be used to train machine learning algorithms to identify and warn them [4]. To ensure responsible and transparent usage of AI technology, the system also suggests establishing strong ethical frameworks and policies to control their research and deployment [5]. Integrating AI ethics into cybersecurity

ISSN 2347–3657
Volume 10, Issue 4, Dec 2022

processes may improve accountability and transparency while enhancing the capacity to identify and prevent exploitation. The suggested approach seeks to safeguard persons and organisations from possible damage by integrating technology improvements with ethical concerns to provide a holistic solution to AI-related crimes.

IV.METHODOLOGY

➢ Data Collection and Literature Review

To have a grasp of the present state of AI crimes and their consequences, the first stage of the technique is to gather extensive data and examine relevant literature. During this stage, we collect information from a wide range of sources, including scholarly articles, reports from businesses, and case studies, with a particular emphasis on cases of AI abuse and misuse. Cybersecurity reports, white papers, and peer-reviewed studies reveal a range of illegal acts with artificial intelligence, such as data breaches, privacy violations, and cyberattacks [1][2]. The purpose of this literature review is to find new dangers, important trends, and research gaps. The many forms of AI crime and the effects they have on people and businesses may be better understood with the aid of this review.

➢ Analysis of Existing Systems

Examining preexisting frameworks and methods for dealing with AI-related criminality is the next stage after the literature assessment. Examining the present state of cybersecurity, privacy laws, and AI-related ethical standards is part of this process. For instance, it will evaluate how well conventional security measures, such intrusion detection systems and firewalls, can identify threats powered by artificial intelligence [3]. Present methods for media verification and privacy protection will also be covered in the examination, with an eye towards assessing their merits and shortcomings in light of AI technology. By doing so, we may see where our present systems are lacking and where we need to look for more tailored answers [4].

➢ Development of AI-Driven Anomaly Detection Models

At this stage of the project, we are creating and deploying models that are powered by AI in order to identify and stop harmful actions. Making machine learning algorithms that can spot out-of-the-ordinary occurrences in digital

ISSN 2347–3657
Volume 10, Issue 4, Dec 2022

information, email conversations, and network traffic is part of this. Take, for example, the ability to train deep learning models like CNNs and RNNs to identify patterns linked to phishing attempts and deepfakes [5][6]. The models will be trained on massive datasets that include instances of both good and bad things to make them more accurate and resilient. The efficacy of these models will be assessed using performance measures including F1-score, recall, and accuracy.

- **Implementation of Ethical Guidelines and Regulations**

At the same time, the initiative will tackle crimes connected to AI by developing a set of ethical norms and regulatory suggestions. It entails looking at current ethical frameworks and suggesting ways to improve them so that AI is used responsibly. Establishing norms for AI systems' openness, accountability, and equity will be the primary emphasis of the suggestions [7]. The project will also suggest new rules or changes to current ones to deal with the unique problems that AI technologies create, such making sure that AI is built and used in a way that doesn't compromise privacy or security [8].

- **Evaluation and Testing**

An extensive testing and assessment procedure will be followed after the development of the AI-driven models and ethical standards. To confirm the models' usefulness in identifying and mitigating AI-related dangers, it is necessary to examine their performance using test datasets and real-world situations. Furthermore, professionals in the area will assess the suggested ethical standards and rules for workability and practicability [9]. Both the technical and regulatory aspects of the project will be fine-tuned and improved based on the comments received from these reviews.

- **Integration and Deployment**

Finally, real-world applications and deployment circumstances should be considered when combining the created AI models and ethical norms. Building integration tools and user interfaces for anomaly detection systems is part of this process [10]. This will help organisations install the systems and follow the standards. To guarantee efficient and problem-free functioning, the deployment will be trialled in test settings. In order to make sure that the new tools and rules are used correctly and adhered to, stakeholders will also be trained on them [11].

ISSN 2347–3657
Volume 10, Issue 4, Dec 2022

- **Continuous Monitoring and Improvement**

There will be a period of ongoing monitoring and improvement of the project after deployment. In order to keep up with emerging threats and the ever-changing tactics employed by bad actors, it is necessary to update the AI models on a regular basis [12]. We will continuously gather input from stakeholders and users to find out what's wrong and how to fix it. Emerging trends and breakthroughs in AI technology will also be taken into account when reviewing and updating the ethical norms and rules [13]. By doing so, we guarantee that the system will continue to tackle AI-related crimes effectively and relevantly.

V.CONCLUSION

In conclusion, there are many advantages to AI technology, but there are also substantial dangers associated with their exploitation or misuse. The many types of AI-related criminality, such as cyberattacks, privacy invasions, and misleading content generation, have been outlined in this research. The initiative draws attention to the need for more sophisticated and AI-specific solutions by examining current systems and their shortcomings. A whole strategy for reducing AI-related criminality is offered by the suggested system, which integrates AI-driven anomaly detection with strong ethical foundations. It is critical to create and execute strong protections to prevent harmful usage of AI and to guarantee its responsible and ethical use as AI technologies advance. Contributing to current efforts to address AI-related dangers and create a safe and ethical AI ecosystem is the purpose of this project's results and suggestions.

VI. REFERENCES

1. Goodfellow, I., Shlens, J., & Szegedy, C. (2015). "Explaining and Improving the Robustness of Classifiers Against Adversarial Examples." *Proceedings of the International Conference on Learning Representations (ICLR)*.

2. Korshunov, P., & Marcel, S. (2018). "DeepFakes: A New Threat to Face Recognition Systems." *Proceedings of the 2018 IEEE International Conference on Image Processing (ICIP)*, 2587-2591.

3. Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.

4. Xu, Y., & Liu, Y. (2019). "Detecting Deepfake Videos with Audio-Visual

ISSN 2347–3657
Volume 10, Issue 4, Dec 2022

Cross-Verification." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2938-2947.

5. Floridi, L. (2019). "The Ethics of Artificial Intelligence." *In The Cambridge Handbook of Artificial Intelligence* (pp. 316-334). Cambridge University Press.

6.Binns, R., & Karthik, S. (2019). "A Survey of Machine Learning Approaches for Detecting Cybersecurity Threats." *Computers & Security*, 87, 101606.

7.Yang, X., & Yang, H. (2020). "Anomaly Detection in Network Traffic: A Deep Learning Approach." *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, 124-130.

8.Cowls, J., & Floridi, L. (2018). "Regulating Artificial Intelligence Systems: Risks, Challenges, and Opportunities." *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency (FAT)*, 54-68.

9.Zhu, J., & Zhou, L. (2020). "AI and the Law: The Role of Artificial Intelligence in Legal Practice." *Journal of Law and Technology*, 22(1), 32-49.

10. Raji, I. D., & Buolamwini, J. (2019). "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products." *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*.