Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.3, May : 2024

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

Mrs. B. Siva Ganga Associate Professor of CSE Department Andhra Loyola Institute of Engineering and Technology Vijayawada, Andhra Pradesh, India sivagangabadipati@gmail.com
V. Geethika Computer Science & Engineering Department Andhra Loyola Institute of Engineering and Technology Vijayawada, Andhra Pradesh, India geethikavadlapudi@gmail.com
B. Reha Computer Science & Engineering Department Andhra Loyola Institute of Engineering and Technology Vijayawada, Andhra Pradesh, India naidusweety76@gmail.com
J. Nissie Diana Computer Science & Engineering Department Andhra Loyola Institute of Engineering and Technology Vijayawada, Andhra Pradesh, India Nissiedianaj@gmail.com

Abstract—

The capabilities of Artificial Intelligence (AI) evolve rapidly and affect almost all sectors of society. AI has been increasingly integrated into criminal and harmful activities, expanding existing vulnerabilities, and introducing new threats. This article reviews the relevant literature, reports, and representative incidents which allows to construct a typology of the malicious use and abuse of systems with AI capabilities. The main objective is to clarify the types of activities and corresponding risks. Our starting point is to identify the vulnerabilities of AI models and outline how malicious actors can abuse them. Subsequently, we explore AIenabled and AI-enhanced attacks. While we present a comprehensive overview, we do not aim for a conclusive and exhaustive classification. Rather, we provide an overview of the risks of enhanced AI application, that contributes to the growing body of knowledge on the issue. Specifically, we suggest four types of malicious abuse of AI (integrity attacks, unintended AI outcomes, algorithmic trading, membership inference attacks) and four types of malicious use of AI (social engineering, misinformation/fake news ,hacking autonomous weapon systems). Mapping these threats enables advanced reflection of governance strategies, policies, and activities that can be developed or improved to minimize risks and avoid harmful consequences. Enhanced collaboration among governments, industries, and civil society actors is vital to increase preparedness and resilience against malicious use and abuse of AI.

Keywords—
Malicious, Crime and abuse on Artificial Intelligence.

I. INTRODUCTION

The impact of Artificial Intelligence (AI) systems has become a focal point in academic studies, political debates, and civil society reports. The development of AI is lauded for its transformative technological capabilities, such as advanced automated image recognition with applications in medicine, like the detection of cancer. However, this technological advancement is not without criticism and apprehension, particularly concerning uncertainties surrounding the consequences of automation on the labor market, including concerns about mass unemployment.AI can be used for good things like helping governments improve their abilities. But at the same time, it can also be used to attack them. So, even though AI can be helpful, it can also cause problems, especially in cybersecurity and fighting cybercrime. The private sector, predominantly driving AI development, extends its applications to customer-oriented domains, while defense sectors utilize similar capabilities for their operations. The line between actions of state and non-state actors is increasingly blurred, as illustrated by recent ransomware attacks targeting public infrastructure in various countries.Moreover, the dual-use aspect of technology is not novel in the realm of cybercrime or cybersecurity. However, the unique vulnerabilities introduced by AI for malicious use and abuse pose novel challenges. The thorough valuation of the threat scenery is vital to initiate and adjust governance mechanisms, tool proactive measures, and bolster cyber resilience.It evaluates the main categories of AI use and abuse in a criminal context, providing illustrative examples to highlight the challenges. The presented typology categorizes the primary harmful AI-based activities, offering a valuable framework for structuring research efforts and pinpointing knowledge gaps. Understanding how people might use AI for bad things helps cybersecurity groups and government agencies get ready to stop those bad things from happening. By learning about these possibilities ahead of time, they can make plans to prevent attacks and stop them fromcausing harm 2

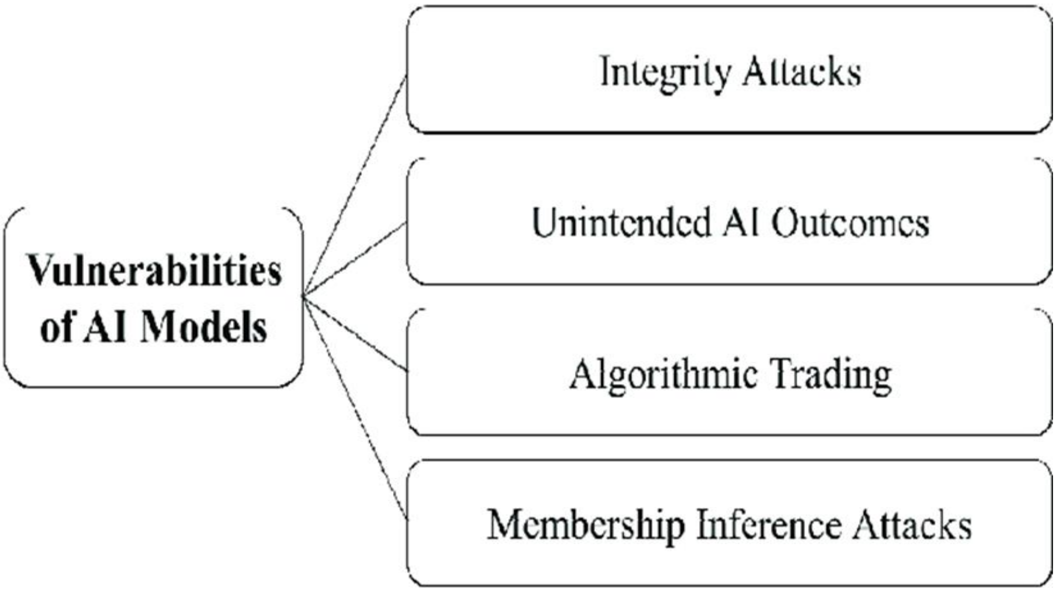
II. LITERATURE SURVEY

Academic studies have delved into the multifaceted impact of AI, addressing its role in areas such as medicine where automated image recognition is applied for tasks like cancer detection . However, the literature also acknowledges the criticisms and concerns, particularly regarding potential repercussions on the labor market, including fears of mass unemployment Political debates have centered around the strategic use of AI by governments to enhance capabilities, raising simultaneous concerns about its exploitation for cyber attacks against these very entities. This dual usage is particularly pronounced in the defense sector, where AI applications intersect with cybersecurity measures.Recent events, like the attack on the Colonial Pipeline Pipeline in the US, show that it's getting harder to tell if an attack is coming from a government or not. This is a big deal because it means anyone, not just governments, can cause serious problems by hacking into important things like public infrastructure. . Moreover, the survey identifies the adaptability of non-malicious programs for malicious intent, emphasizing the dual-use aspect of technology in the cybercrime landscape.While acknowledging that the dual-use nature of technology is not entirely novel in cybersecurity, the literature emphasizes how AI introduces novel vulnerabilities. Ongoing assessments of the threat landscape are deemed crucial, necessitating the establishment and adaptation of governance mechanisms, the implementation of proactive measures, and the enhancement of cyber resilience.The typology presented in this survey categorizes harmful AI-based activities, offering a valuable framework for organizing research efforts and identifying gaps in knowledge that warrant further investigation. The insights derived from this literature survey equip cybersecurity organizations and governmental agencies with the knowledge needed to anticipate, prepare for, and mitigate potential malicious use and abuse of AI in the cyber domain

III PROBLEM STATEMENT EXISTING SYSTEM:

PROPOSED SYSTEM: Positive Aspects: Technological Advancements: AI is celebrated for its transformative technological capabilities, particularly in applications like automated image recognition for tasks such as cancer detection in the field of medicine The typology presented in this paper aims to contribute to several important aspects within the field of AI's impact on cybersecurity and cybercrime: Knowledge Enhancement. Interdisciplinary Collaboration. Mitigation Strategies and Collective Effort. ADVANTAGES: • By concentrating on these objectives, the system strives to construct a nuanced typology firmly grounded in the ongoing debate and substantiated by empirical evidence. The emphasis is on identifying and categorizing the essential components that define the malicious use and abuse of AI, particularly in the context of compromising data availability, confidentiality, and integrity. • The intentional delineation of these goals ensures a focused and comprehensive exploration, allowing for a detailed analysis of real-world instances where AI systems are manipulated for malicious ends. This approach positions the system to contribute valuable insights to the ongoing discourse surrounding AI technologies and their potential vulnerabilities in terms of data security

IV RESULT FOR PROPOSED SYSTEM



The diagram delineates the multifaceted landscape of malicious abuse within the realm of Artificial Intelligence (AI), encapsulating four distinct categories: integrity attacks, unintended AI outcomes, algorithmic trading, and membership inference attacks. The representation begins with an illustration of integrity attacks, 3 symbolized by a broken chain, signifying the compromise of data integrity. Algorithmic trading is depicted through financial symbols, underscoring the manipulation of AI algorithms in financial markets and the associated potential for disruptions and unfair advantages,

V. RESULTS & DISCUSSION

In the system's architecture, various user roles interact with distinct functionalities. The Service Provider, upon successful login, gains access to operations such as browsing datasets, training and testing data sets, and visualizing accuracy through bar charts. Detailed results and metrics are available, including the prediction of crime types and the visualization of crime type ratios. Additionally, the Service Provider can download datasets containing predicted crime types and oversee all registered Remote Users. The Admin, operating within a separate module, possesses the authority to view and authorize users. On the other hand, Remote Users are required to register before utilizing functionalities like predicting crime types and managing their profiles. This modular approach ensures a streamlined and role-specific experience, catering to the diverse needs of Service Providers, Admins, and Remote Users within the system

VI. CONCLUSION

Understanding the risks that come with using and misusing AI systems is really important. It helps us figure out how to keep society and critical infrastructures safe from possible attacks, Based on what we've read and studied, we're focused on creating a system to classify how bad guys could use AI to cause different kinds of harm. This includes physical, mental, political, and economic harm. We're also looking into how AI models can have weaknesses and how AI can be used in attacks, like making fake stuff. All of this helps us understand the challenges we're facing. Notable incidents like the 2010 flash crash and the Cambridge Analytica scandal underscore the real-world implications of these threats, while experimental showcases like IBM's Deep Locker In response to the risks identified, we've outlined potential mitigation strategies. Collaboration among industries, governments, civil society, and individuals is paramount, involving the development of knowledge, awareness, and technical/operational systems to effectively address the challenges posed by the malicious use of AI. While the classification presented serves as a valuable starting point, it acknowledges its limitations, as certain AI-enabled or AI-enhanced attacks may not neatly fit into established categories. Future work should leverage empirical methods to assess the generalizability and representativeness of the classification scheme, and statistical analysis, when supported by sufficient data, could provide a more comprehensive overview of the threat landscape. Continuous mapping of risks associated with the malicious use and abuse of AI is imperative, enhancing preparedness and bolstering the capacity to prevent and respond effectively to potential attacks.

VII. FUTURE WORK:

Future work in the domain of AI security and ethical considerations should embark on several critical pathways to effectively address the evolving challenges posed by the malevolent use and misuse of AI. One imperative avenue involves the development of advanced classification models that can dynamically categorize emerging threats, adapting to the rapidly evolving landscape of AI misuse. Empirical validation studies are essential to assess the effectiveness and generalizability of existing classification schemes, leveraging real-world incidents to ensure comprehensive coverage of diverse AIrelated threats. Furthermore, establishing comprehensive ethical guidelines and governance frameworks for AI development, deployment, and usage is paramount, necessitating collaboration between industry, academia, policymakers, and civil society to establish universally accepted standards. Enhanced awareness and education initiatives are crucial for empowering individuals and organizations to make informed decisions and implement responsible AI practices. Continuous monitoring systems, supported by real-time analytics and threat intelligence, should be implemented to stay ahead of evolving risks. International collaboration is vital to address the global nature of AI-related threats, fostering frameworks for information sharing, coordinated responses, and harmonized regulatory approaches. Research into human-AI interaction dynamics, privacy-preserving AI technologies, and impact assessment methodologies is essential for understanding the psychological, social, and economic implications of AI misuse. Finally, regulatory innovation is needed to ensure that regulatory

frameworks remain agile and adaptive, keeping pace with the rapid advancements in AI technology and effectively addressing novel challenges in the ethical use of AI. By prioritizing these areas, stakeholders can contribute to a more secure, responsible, and ethically grounded AI ecosystem

VIII. REFERENCE

[1] K. Crawford, Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. London, U.K.: Yale Univ. Press, 2021.

[2] D. Garcia, ``Lethal arti_cial intelligence and change: The future of international peace and security,'' Int. Stud. Rev., vol. 20, no. 2, pp. 334_341, Jun. 2018, doi: 10.1093/isr/viy029.

[3] T. Yigitcanlar, K. Desouza, L. Butler, and F. Roozkhosh, ``Contributions and risks of arti_cial intelligence (AI) in building smarter cities: Insights from a systematic review of the literature,'' Energies, vol. 13, no. 6, p. 1473, Mar. 2020, doi: 10.3390/en13061473.

[4] I. van Engelshoven. (Oct. 18, 2019). Speech by Minister Van Engelshoven on Arti_cial Intelligence at UNESCO, on October the 18th in Paris. Government of The Netherlands. Accessed: Apr. 15,2021[Online].Available:https://www.government.nl/documents/s peeches/2019/10/18/speech-by-minister-van-engelshoven-onarti_cial-intelligence-atunesco

[5] O. Osoba andW.Welser IV, The Risks of Arti_cial Intelligence to Securityand the Future of Work. Santa Monica, CA, USA: RAND Corporation,2017, doi: 10.7249/PE237.

[6] D. Patel, Y. Shah, N. Thakkar, K. Shah, and M. Shah, ``Implementation ofarti_cial intelligence techniques for cancerdetection,'' Augmented Hum.Res., vol. 5, no. 1, Dec. 2020, doi: 10.1007/s41133-019-0024-3.

[7] A. Rodríguez-Ruiz, E. Krupinski, J.-J. Mordang, K. Schilling, S. H. Heywang-Köbrunner, I. Sechopoulos, and R. M. Mann, ``Detectionof breast cancer with mammography: Effect of an arti_cial intelligence support system,'' Radiology, vol. 290, no. 2, pp. 305_314, Feb. 2019,doi: 10.1148/radiol.2018181371.

[8] J. Furman and R. Seamans, ``AI and the economy," Nat. Bur. Econ. Res., NBER, Cambridge, MA, USA,Work. Paper, 2018, doi: 10.3386/w24689.

[9] D. R. Coats, Worldwide Threat Assessment of the U.S. Intelligence Com-munity. New York, NY, USA, 2017, p. 32.

[10] L. Floridi, ``Soft ethics: Its application to the general data protectionregulation and its dual advantage," Philosophy Technol., vol. 31, no. 2, pp. 163_167, Jun. 2018, doi: 10.1007/s13347-018-0315-5.

[11] P. S. Chauhan and N. Kshetri, ``2021 state of the practice in data privacy and security," Computer, vol. 54, no. 8, pp. 125_132, Aug. 2021, doi:10.1109/MC.2021.3083916

[12] S. Gordon and R. Ford, ``On the de_nition and classi_cation of cybercrime,"J. Comput. Virol., vol. 2, no. 1, pp. 13_20, Aug2006, doi:10.1007/s11416-006-0015-z.