International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

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

K. Aarati [1], A. Swathi Likhitha [2], A. Srinitha[3], B. Samatha[4], B. Spanadana[5]

[1] Assistant Professor, Department of CSE, Malla Reddy Engineering College For Women Hyderabad, Telangana, India

[2,3,4,5] UG Scholar, Department of CSE, Malla Reddy Engineering College For Women Hyderabad, Telangana, India

mrecwaarati27sep@gmail.com
likhithaswathi254@gmail.com,patelsrinitha@gmail.com,samathabandari12@gmail.com,
bathinenispandana91@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 AI-enabled 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 ofmalicious 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.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

INTRODUCTION

Machine learning is an important component of the growing field of data science. Through the use of statistical

methods, different type of algorithms is trained to make classifications or predictions, and to uncover key insights in this project. These insights subsequently drive decision making within applications and businesses, ideally impacting key growth metrics.

Machine learning algorithms build a model based on this project data, known as training data, in order to make predictions or decisions without being explicitly programmed to do so. Machine learning algorithms are used in a wide variety of datasets, where it is difficult or unfeasible to develop conventional algorithms to perform theneeded tasks.

The impact of systems using Artificial Intelligence (AI) is at the center of numerous academic studies [1]_[3], political debates [4], and reports of civil society organizations [5]. The development of AI has become the subject of praise due to unprecedented technological capabilities, such as enhanced possibilities for automated image recognition (e.g., detection of cancer in the field of medicine [6], [7]). However, it has also been criticized - even feared - due to aspects such as the uncertain consequences of automation for the labor market (e.g., concerns of mass unemployment [8, pp. 26_27]). This duality of positive *vs* negative aspects of the technology can also be identified in the context of cybersecurity and cybercrime. Governments use AI to enhance their capabilities, whereas the same technology can be used for attacks against them [9].

While the recent surge in AI development has been fueled by the private sector and applications in customer-oriented applications, sectors such as defense might use similar capabilities in their operations [10]. At the same time, it is increasingly difficult to distinguish between the actions of state and non-state actors. This has recently been demonstrated by a wave of ransomware attacks targeting public infrastructure in many countries, such as the Colonial Pipeline in the United States in May 2021 [11, pp. 127_128]. Additionally, programs and applications developed for non-malicious purposes can also be implemented or modified for malicious intent and potentially cause

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

harm. The dual-use aspect of technology is not an entirely new problem when it comes to cybercrime1 or (cyber-
)security. Nevertheless, how AI can be leveraged for malicious use and abuse constitutes novel vulnerabilities. Permanent assessment of the threat landscape is crucial to create and adapt governance mechanisms, develop proactive measures, and enhance (cyber-

)resilience. To build on previous work [14]_[16] and expand the understanding of how AI broadens the potential for malicious activities online, this article evaluates the main categories of use and abuse of AI in a criminal context.We provide several salient examples that allow us to illustrate the challenges at hand. Based on these examples, we present a typology that catalogs the main harmful AI-based activities. Developing knowledge and understanding about the potential malicious use and abuse of AI enables cybersecurity organizations and governmental agencies to anticipatesuch incidents and increase their preparedness against attacks. Furthermore, a typology is greatly useful in structuring research efforts and identifying gaps in knowledge in areaswhere more research is warranted.

EXISTING SYSTEM

To build on previous work [14]_[16] and expand the understanding of how AI broadens the potential for malicious activities online, this article evaluates the main categories of use and abuse of AI in a criminal context.We provide several salient examples that allow us to illustrate the challenges at hand. Based on these examples, we present a typology that catalogs the main harmful
AI-based activities. Developing knowledge and understanding about the potential malicious use and abuse of AI enables cybersecurity organizations and governmental agencies to anticipatesuch incidents and increase their preparedness against attacks. Furthermore, a typology is greatly useful in structuring research efforts and identifying gaps in knowledge in areaswhere more research is warranted.

Disadvantages

- An existing methodology not proposed the term ``AI-Crime'' to describe the situation in which AI technologies are re-oriented to facilitate criminal activity.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

- An existing system doesn't implement for MALICIOUS ABUSE OF AI and VULNERABILITIES OF AIMODELS.

Proposed System;

With the typology presented in this paper, we hope to make the followingcontributions:

a. Add to the emerging body of knowledge that maps types of malicious use and abuse of AI systems. To understand the main concepts, threat scenarios, and possibilities is necessary to develop much-needed preventive measures and proactive responses to such attacks.

b. Help in establishing a shared language among and across different disciplines, especially between STEM disciplines and legal practitioners, as well as policymakers. Interdisciplinary research on the topic can reduce confusion caused by excessively technical or monodisciplinary language and aid in bridging existing gaps.

c. Propose mitigation strategies, as well as demonstrating that a collective effort among government, academia, and industry is needed.

The methodology is based on an analysis of the available literature on cybercrime and the potential malicious use and abuse of AI systems. A literature review informs this study and findings using the following databases: IEEE Xplore, Science Direct, Wiley Online Library, and Google Scholar. We used keywords, titles, and screened abstracts. The search terms included are (Artificial Intelligence OR AI OR Machine Learning OR ML) AND (malicious OR crime OR harmful OR cyber attack). Additionally, we examined lists of references obtained from reviewed papers and reports, as well as news sources describing past AI incidents. We only reviewed

papers/reports/web pages available in English and Portuguese. After analyzing these sources, we were able to identify the different types of malicious use and abuse of AI systems.

Machine learning (ML) has become more prevalent in recent years. This has created

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

incentives for attackers to manipulate models (e.g., the software itself) or the underlying data, making ML models prone to integrity attacks. In integrity attacks, hackers attempt to inject false information into a system to corrupt the data, undermining their trustworthiness.

Advantages

- The system aims to propose a typology of the malicious use and abuse of AI based on empirical evidence and contemporary discourse, analyzing how AI systems are used to compromise confidentiality, integrity, and data availability.
- Objectives are limited toidentifying essential elements of the malicious use and abuse of AI, and to collect evidence of their use in practice. The compiled data enable furtheranalysis of the possible ways in which AI systems can be exploited for criminal activities.

IMPLEMENTATION

Service Provider

In this module, the Service Provider hasto login by using valid user name andpassword. After login successful he cando some operations such as Login,Browse Datasets and Train &Test Data Sets ,View Trained and TestedAccuracy in Bar Chart ,View Trainedand Tested Accuracy Results ,View,Prediction Of Crime Type ,View Crime Type Ratio ,Download Predicted Data Sets ,View Crime Type Ratio Results ,View All Remote Users

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

LOGIN, PREDICT CRIME TYPE,VIEW YOUR PROFILE.

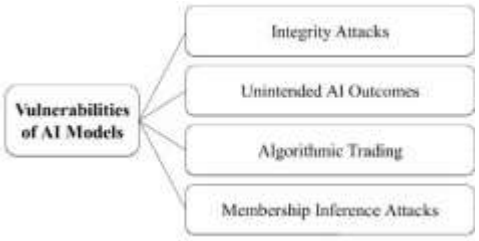

Fig.1. Malicious Abuse of AI

Fig.2. . Malicious Use of AI.

CONCLUSION

The threats posed by the use and abuse of AI systems must be well understood to create mechanisms that protect society and critical infrastructures from attacks. Based on the available literature, reports, and previous incidents, we focused on creating a classification of how AI systems can be used or abused by malicious actors. This includes, but is not limited to, physical, psychological, political, and economic harm. We explored the vulnerabilities of AI models, such as unintended outcomes, and AI-enabled and AI-enhanced attacks, such as forgery. This article also describes past incidents, such as the2010 _ash crash and the Cambridge

Analytica scandal, manifesting the challenges at hand.We also outlined attacks that, to the best of our knowledge, have only been demonstrated through ``proof of concept'', such as IBM's DeepLocker. In response to the risks presented in this paper, we have also explored some possible mitigation strategies. Industries, governments, civil society, and individuals should cooperate in developing knowledge and raising awareness while developing technical and operational systems and procedures to address the challenges.

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Although this type of classification is a useful starting point, it does not come without drawbacks. Some AI-enabled or AI-enhanced attacks might not fit the categories established. Further work could use empirical methods to assess whether the classification scheme presented is generalizable and representative. When sufficient data is available, methods such as statistical analysis could be helpful to reach a more complete overview of the threat scenario. Continuously mapping the risks associated with malicious use and abuse of AI helps to enhance preparedness and increases the potential to prevent and adequately respond to attacks.

REFERENCES

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

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.

T. Yigitcanlar, K. Desouza, L. Butler, and F. Roozkhosh, ``Contributions and risks of arti_cial intelligence (AI) inbuilding smarter cities: Insights from a systematic review of theliterature," Energies, vol. 13, no. 6, p. 1473, Mar. 2020, doi:10.3390/en13061473.

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-on-arti_cial-intelligence- atunesco

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

D. Patel, Y. Shah, N. Thakkar, K. Shah, and M. Shah, ``Implementation of arti_cial intelligence techniques for cancer detection," Augmented Hum. Res., vol. 5, no. 1, Dec. 2020, doi:10.1007/s41133-019-0024-3.

A. Rodríguez-Ruiz, E. Krupinski, J.-

International journal of basic and applied research
www.pragatipublication.com
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

J. Mordang, K. Schilling,
S. H. Heywang-Köbrunner, I.Sechopoulos, and R. M. Mann, ``Detection
of 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.
J. Furman and R. Seamans, ``AI and the economy," Nat. Bur. Econ. Res., NBER, Cambridge, MA, USA,Work.Paper, 2018, doi: 10.3386/w24689.
D. R. Coats, Worldwide Threat Assessment of the U.S. Intelligence Com-
munity. New York, NY, USA, 2017, p. 32.
L. Floridi, ``Soft ethics: Its application to the general data protection regulation and its dual advantage," Philosophy Technol., vol. 31, no. 2,
pp. 163_167, Jun. 2018, doi: 10.1007/s13347-018-0315-5.