International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

Artificial Intelligence Crime : An Overview of Malicious Use and Abuse of AI

***[1]Mehveen Mehdi Khatoon, B Manaswi Varma[2], P Hima Bindu[3]**
[1]Associate Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India
[2,3]Students, Department of Information Technology, Bhoj Reddy Engineering College for Women, Hyderabad, India

ARTICLEINFO

Article History:
Accepted: 05 April 2023
Published: 28 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
966-970

ABSTRACT

Artificial Intelligence (AI) advances have affected nearly every subject, including computer science, criminology, robotics etc Because of AI's outstanding ability to acquire and analyse vast amounts of data, its methodologies are suitable for tackling a range of crime-related issues. Despite the fact that AI has solved a variety of problems, AI experts have warned about the possible security risks associated with AI algorithms and training data. As AI systems inherit existing computer system security concerns, concern about unique cyberattacks aided by AI is growing. This work review literature assessment on security risks and AI-related criminality in this setting. Based on the literature analysis, this article defines AI crime and divides it into two categories: tool crime and target crime. In addition, forensic approaches are discussed. We also look at the features of AI crimes in the past and now. Traditional forensic approaches are unable to tackle problems that are tough to solve. Finally, there are some unresolved difficulties discussed, with a focus on the need to develop new AI forensics tools.

Keywords : Artificial Intelligence, AI Crimes, Forensic

I. INTRODUCTION

AI has the ability to acquire and analyse vast amounts of data, its methodologies are suitable for tackling a range of crime-related issues. Many people are interested in AI cyber security because it is a popular and relevant scientific issue. The concerns we will encounter will include not just pure science and technology issues, but also political and social influence challenges that will cause issues in our society. Therefore AI is every import and subject in every field like computer science, criminology, robotics etc Deep Learning, which is inspired by the structure and function of the brain, has been a key accomplishment in the AI area, igniting AI research in a variety of fields. Deep learning research has been investigated to handle large amounts of data (e.g., photos, social media, crime data information, and so on) in order to do medical picture analysis, speech analysis, and so on. While AI's rapid progress has

provided benefits in terms of innovation, it has also come with considerable concerns. Unexpected problems (e.g., terrorism, security threats, cybercrime, privacy violation, etc.) arose when ICT advanced at fast speeds in the past, resulting in significant social costs. Similarly, there are rising concerns about the potential for AI to generate a variety of issues. We look at AI security concerns, predictable crimes, and digital forensics for AI in this context. After defining AI crime, we offer a taxonomy for new sorts of crime: the AI as tool crime and AI as target crime, inspired by an existing taxonomy [1] used in cybercrime: Computer as tool crime and computer as target crime.

II. RELATED WORK

Various academics has already analyzed AI. From many viewpoints, this section discusses studies on the AI security threat and AI-related criminality. We also look at cybercrime as defined by the cybersecurity and digital forensics communities.

2.1 AI security threads and crime

Because the term 'crime' is associated with law and ethics, the phrase 'AI crime' was originally coined by the humanities sector. Several research have highlighted security dangers and malevolent applications of AI that can cause numerous crimes, despite the fact that the phrase AI crime has not been explored in the computer science field. The concerns we will encounter will include not just pure scientific and technological issues, but also political and social impact challenges that will cause troubles in our society. Many contemporary issues and concerns about AI security have been documented, by some recent investigation and conversations. Adopting online identities, known as socialbots, that behave like humans is a great example of harmful AI use. Though the original goal of socialbot was to promote awareness and collaboration among people, it has been used negatively in the past for phishing, fraud, and political infiltration into online social networks campaigns [2]. Machine learning, according to Seymour and Tully [6], can be used for social engineering; for example, using AI, mass-produced tweets with phishing links could be broadcast on Twitter without causing any disruption. Because the harmful socialbot is based on a specific user's previous actions and public profiles, detecting it has become a computer security issue. When harmful socialbots are created to carry out a political attack, the tactic may affect or inflame public opinion, according to social science [3] [4]. According to some academics, hackers have already begun to weaponize AI in order to improve their hacking abilities and develop new sorts of cyber attacks [5]. Traditional cybercrimes such as financial fraud, cyber terrorism, and cyberextortion are all using AI to improve their strategies. Unlike the above research, which focused on the difficulties that certain techniques could cause, Brundage et al. [6] provided a holistic view of AI's malevolent use. They focused on three shifts in the threat landscape: the growth of current risks, the introduction of new threats, and a shift in the threat's characteristic character. The cost of jobs that require human labour could be reduced thanks to the AI system's scalability. As a result of the cost-cutting strategies (e.g. mass spear phishing), perpetrators are able to attack more targets, resulting in the expansion of existing dangers. New dangers may also arise to fulfil jobs that are impossible for humans to complete (for example, impersonating individual voices or commanding many drones). The normal character of threats will be altered when highly effective AI strikes become increasingly widespread. Security domains were also divided into three categories by Brundage et al.: digital security, physical security, and political security. Cyberattacks that target human or AI systems are included in the digital security realm. Physical threats, such as forcing autonomous vehicles to crash and manipulating thousands of drones, are under the physical security realm. New dangers in profiling, repression, and targeted disinformation efforts are all part of the political security arena. By introducing the phrase 'AI crime,' King et al. [7] gave

a distinct perspective on AI security issues. They looked at the issue from a different angle. Commerce, financial markets, and insolvency (e.g. market manipulation, price fixing, collusion), harmful or dangerous drugs (e.g. trafficking, selling, buying, possessing banned drugs), offences against the person (e.g. harassment, torture), sexual offences (e.g. sexual assault, promotion of sexual offence), theft and fraud, and forgery and personation are all classified as AI crimes in the article (e.g. spear phishing, credit card fraud). They argued that the offences are classified as having one or more threats. They focused on human nature when identifying AI security threats: emergence, liability, monitoring, and psychology. The psychology threat, for example, implies that AI can influence a human's mental state to the point of aiding or instigating crime. This approach differs significantly from that of computer science; this diversity of viewpoints is due to AI's inherent inter disciplinarity. Some research has focused on AI privacy concerns emerging from the processing of personal data.According to Li and Zhang [8], AI applications in healthcare, banking, and education may cause privacy issues. Because the quantity and quality of training data have a significant impact on AI performance, developers want to acquire as much data as possible. The acquisition of extensive data, according to Li et al., has inherent privacy risks. Mitrou [9] used the General Data Protection Regulation to tackle the issue of privacy (GDPR). Although GDPR does not expressly address AI, the author emphasised that it can be applied to AI when it manages personal data. The prior research has three consequences for AI stakeholders. First, due to AI's dual-use nature, researchers and engineers should be aware that the technology could be used to execute criminal acts, even if it was created for legal purposes. Second, completely new forms of security risks will develop that have never been considered before. Because AI can do activities that were previously thought to be impossible for people or traditional programmes to complete, the threats will be outside the core purview of known threats. To prevent AI security threats and respond to AI crime, AI researchers should interact closely with specialists from other industries. Finally, the AI security field should learn from the cybersecurity industry's mistakes. The anticipated AI crimes are very intimately involved in cybercrime, as reported in prior studies. The dual-use nature of ICT led to cybercrime; the current state of AI security mimics the early stages of cyber security.

2.2 Cybercrime

Cybercrime is seen as the evil side of the internet.It is divided into two types: computer as target crime and computer as tool crime[10][11]. New sorts of crimes, such as cyberterrorism, cyberextortion, and cyberwarfare, have evolved as information has become digitised and connected via network; these crimes are known as computer as target crime. The goal of computer-as-a-target crime is to disable or destroy computer systems. As a result, when criminals execute a computer-as-a-target crime, they employ tools or procedures that have been created to break into computer systems. In the meantime, every data in our daily lives has been digitised, from personal to professional. Offline crimes like as fraud, threats, child abuse, stalking, and so on now enter the online world as a result of this transformation. It is known as computer as a tool crime in the online world. The taxonomy of cybercrime has aided in the development of practical measures to combat the crime. When forensic investigators look into computer-as-a-tool crime, they focus on demonstrating the perpetrator's previous conduct to see if any illegal activity has place. Criminals that utilise computers as tools typically use well-known technologies and manipulate well-known infrastructures such as text messages, websites, social media, and so on. When investigating a computer as a target crime, however, detectives should concentrate on malicious applications, sometimes known as malware. To respond promptly to the crime and determine the amount of the damage, they must first

locate the malware and then undertake reverse engineering to determine the virus's purpose and the source of the attack. [12] [13]

III. PROPOSED SYSTEM

There have been major technological advancements that have impacted cybersecurity. One of the main game changers in the area of cybersecurity is the development of tools and methods that are supplemented as a sub-group by artificial intelligence (AI) [13]. Artificial Intelligence (AI) is no longer simply a trendy term; it is now being utilized widely across a wide range of sectors. Customer support, healthcare, and robotics are just a few of the many areas where AI has accelerated progress [13]. Additionally, it is making a major contribution to the continuing combat against cybercrime. Here are a few ways AI is helping to improve cyber security.

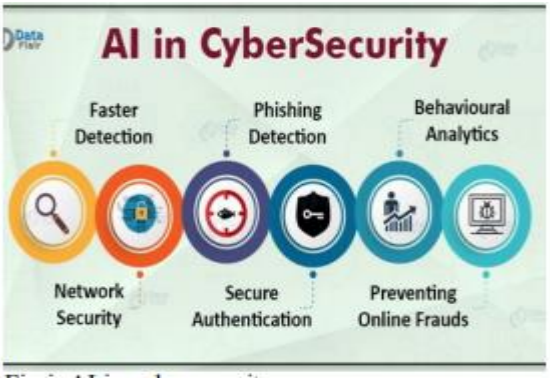

Fig 1 : AI in cyber security

AI has numerous benefits and uses in several domains, including cyber security. With rapidly changing cyber-attacks and the rapid increase of gadgets nowadays, AI can help keep cybercriminals alert, automate threat detection and react more efficiently than standard software and manual methods [14]. Here are some benefits and uses for cyber security use of AI

IV. CONCLUSION

This study evaluated the impact of artificial intelligence on cyber security and the mitigation of cyber security threats. The findings suggest that technological developments have made it simpler for hackers to enhance their tactics, methods, and instruments to abuse people and organizations. While artificial intelligence is beneficial, it also has the potential to be harmful. Selecting technology wisely will enable businesses to avert a crisis. Artificial intelligence (AI) is quickly becoming a must-have tool for improving the effectiveness of information security organizations. Humans are no longer capable of adequately securing an enterprise level attack surface, and artificial intelligence provides the much-needed monitoring and threat detection that can be utilized by security experts to reduce the likelihood of a breach and improve their organization's defense capabilities. Furthermore, artificial intelligence may assist in the discovery and prioritization of risks, the direction of incident response, and the identification of malware cyber-attacks before they occur. As a result, even with the possible drawbacks, artificial intelligence will aid to advance cyber security and assist businesses in developing a stronger overall security.

V. REFERENCES

[1]. D. Cole, "Artificial intelligence and personal identity", Synthese, vol. 88, no. 3, pp. 399-417, 1991. Available: 10.1007/bf00413555.

[2]. M. Stefik, "Artificial intelligence applications for business management", Artificial Intelligence, vol. 28, no. 3, pp. 345-348, 1986. Available: 10.1016/0004-3702(86)90055-x.

[3]. G. Babu, N. Anandakuma and D. Muralidhar, "Countermeasures Against DPA Attacks on FPGA Implementation ofAES", Journal of Artificial Intelligence, vol. 5, no. 4, pp. 186-192, 2012.

[4]. G. Qin, T. He and J. Chen, "Model of preventing URL attacks based on artificial immunity", Journal of Computer Applications, vol. 32, no. 5, pp. 1400-1403, 2013.

[5]. N. Lee, “Artificial Intelligence and Data Mining,” Counterterrorism and Cybersecurity, pp. 323–341, 2015.

[6]. L. Shellberg, "A Cyber Chase in Cyber Space: How International Law Must Address the Threat of Cyber Attacks or Suffer the Consequences", SSRN Electronic Journal, 2013.

[7]. H. R. Nemati, Information security and ethics: concepts, methodologies, tools, and applications. Hershey Pa.: Information Science Reference, 2008.

[8]. T. Tagarev, "Intelligence, Crime and Cybersecurity", Information & Security: An International Journal, vol. 31, pp. 05-06, 2014.

[9]. R. Winkels, Eleventh International Conference on Artificial Intelligence and Law: proceedings: June 4-8, 2007, Stanford Law School, Stanford, California. Place of publication not identified: ACM, 2007.

[10]. D. Hutchison, M. Atiquzzaman, H.-H. Chen, T. Kanade, T.-hoon Kim, J. Kittler, J. M. Kleinberg, C. Lee, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. P. Rangan, J. H. Park, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, and S.-S. Yeo, Advances in Information Security and Assurance. Berlin, Heidelberg: Springer Berlin Heidelberg.

[11]. M. Zajko, "Canada’s cyber security and the changing threat landscape", Critical Studies on Security, vol. 3, no. 2, pp. 147-161, 2015.

[12]. R. Winkels, Eleventh International Conference on Artificial Intelligence and Law: proceedings: June 4-8, 2007, Stanford Law School, Stanford, California. Place of publication not identified: ACM, 2007.

[13]. H. Bidgoli, Handbook of information security. Hoboken, NJ: JohnWiley, 2006.

[14]. H. Zhuge, "Semantic linking through spaces for cyber-physical-socio intelligence: A methodology", Artificial Intelligence, vol. 175, no. 5- 6, pp. 988-1019, 2011.

[15]. C. Blackwell and H. Zhu, Cyberpatterns: Unifying Design Patterns with Security and Attack Patterns, 2nd ed. Cham : Springer International Publishing, 2014.

Cite this article as :

Mehveen Mehdi Khatoon, B Manaswi Varma, P Hima Bindu, "Artificial Intelligence Crime : An Overview of Malicious Use and Abuse of AI", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 10 Issue 2, pp. 966-970, March-April 2023.

Journal URL : https://ijsrst.com/IJSRST52310254