IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

Cyber Crime and Artificial Intelligence – Unleashing A New Era of Menacing Cyber Attacks

Dr. K. Kanchana[1], Ms. Aasiya Parveen S[2], Ms. Deepika B[3] and Ms. Kaviya P[4]
M. Com., Ph.D., (NET & SET), Department of B. Com. (CS)[1]
III B. Com. Corporate Secretaryship[2,3,4]
Chevalier T. Thomas Elizabeth College for Women, Chennai, Tamil Nadu, India

Abstract: *Artificial Intelligence (AI) is a buzz word in the cyber world. Artificial Intelligence is ruling across sectors and nations. Artificial Intelligence and Cyber security intersect with each other in wide range of inter-disciplinary approach. Large corporations are investing in AI and funding from venture capital and private equity funds is growing rapidly. Digital infrastructure and highly trained manpower are the primary keys to manage the transition while companies adopting for AI technologies. This persuades the necessity for upskilling the existing workforce to create technology-infused platforms. This study is a quantitative based research with primary data collected from the general public working in various sectors. An attempt was taken to analyse various AI powered cyber attacks and offer possible security measures to alert the citizens in today's highly threatening cyber world. Without strong security measures, AI is meaningless as it can be easily accessible by others.*

Keywords: Artificial Intelligence, Cyber security and Digital Infrastructure

I.INTRODUCTION

Artificial intelligence AI is catching a lot of headlines recently. There are so many applications of AI that we use in our day to day lives without even knowing it. Such as, Siri, Alexa, Self-driven cars, Robotics, Gaming etc. Large language models LLMs AND generative AI applications like OpenAI's ChatGPT, Microsoft's Bing Chat have given wide access to all and capture our minds by creating jaw-dropping creativities this might also pose a threat to a lot of people. As technology plays an increasingly influential role in our lives, the threat of cybercrime poses a significant challenge to individuals, businesses, and governments worldwide. Since everyone has access to these tools, nothing is stopping cyber criminals from utilizing AI's advanced capabilities to their benefit. AI is a broad and complex field, but in the simplest term, it refers to a machine's ability to combine computers, datasets and sets of instructions to perform tasks that usually require human intelligence, such as reasoning, learning, decision-making and problem-solving. Cyber-criminals may use AI for malicious purposes as well.

1.1 OBJECTIVES THE STUDY

The following objectives are undertaken in this study:
1. To know the various AI tools and its significance in cyber security.
2. To measure the impact of AI tools in identifying the different cyber attacks.
Some ways AI can be used in cybercrime are:
The **Council of Europe Convention on Cybercrime** has defined cybercrime as offenses against confidentiality, integrity, and availability of computer data and systems, computer-related offenses, and content-related offenses, including copyright infringement and data interception.

1.2 AI-Powered Cyber-attacks

a) Deepfakes

Deepfake is a combination of "deep learning" and "fake media," referring to the use of AI to craft/manipulate audio/visual media to appear authentic. Cybercriminals already use this technology to craft non-consensual pornography of celebrities or spread political misinformation and even tricked a UK-based energy firm into transferring €220,000 to a Hungarian bank account in 2019.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

b) AI-Powered Password Cracking

Cybercriminals are employing machine learning ML and AI to improve algorithms for guessing users' passwords. While some password-cracking algorithms already exist, cybercriminals will be able to analyze large password datasets and generate different password variations.

c) Potential AI-Assisted Attacks Targeting Businesses

As you can see, cybercriminals are already using AI to their advantage. Here are some potential AI-powered cyberattacks that may affect your business.

d) Business Email Compromise BEC

A business email compromise is a type of phishing attack targeting organizations to steal money/critical information. AI algorithms can analyze communication patterns and generate convincing phishing emails that impersonate high-level executives or business partners, aiming to deceive employees into performing unauthorized actions like initiating fraudulent transactions or disclosing sensitive information.

e) Advanced Persistent Threats APTs

APTs use sophisticated techniques to breach business networks, remain undetected and exfiltrate sensitive information over an extended period. AI algorithms enable attackers to adapt their tactics, evade security measures and exploit vulnerabilities in business systems.

f) Ransomware Attacks

Ransomware encrypts business-critical data and demands a ransom for decryption codes. AI algorithms can automate and enhance ransomware distribution and selectively target valuable assets, increasing the potential payout for cybercriminals.

g) Fraudulent Transactions

Scammers can employ sophisticated AI algorithms to automate fraudulent transactions targeting businesses. AI-driven fraud can mimic legitimate transaction patterns to evade traditional fraud detection systems and exploit weaknesses in payment processes.

h) Payment Gateway Fraud

Cybercriminals may utilize AI technology to automate and leverage various aspects of payment gateway fraud, making it more sophisticated and challenging to detect. Fraudsters may employ techniques like generating realistic synthetic identities, analyzing patterns to evade detection systems or conducting targeted phishing attacks using AI-generated content.

i) Distributed Denial Of Service DDoS Attacks

AI can enhance the scale of intensity of DDoS attacks against business websites and online services. AI-powered botnets can coordinate massive volumes of malicious traffic, overwhelming servers and disrupting business operations.

j) Intellectual Property Theft

AI can help cybercriminals automate the process of targeting businesses to steal valuable intellectual property. AI algorithms can analyze high-volume of data and identify high-value trade secrets or sensitive information, facilitating their theft for competitive advantage or financial gain.

k) Wrap-Up

The emergence of artificial intelligence has provided cybercriminals with powerful tools to carry out attacks with greater efficiency and sophistication. The threats will keep getting more and more sophisticated with each development. Safeguarding businesses against these threats calls for an advanced, multi-faceted approach that combines advanced AI-

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

driven cyber-security solutions combined with experience cyber-security experts and a proactive stance against threat response. There are a lot of concerns with how AI can enhance crimes," he said. "But we can also use AI to investigate."

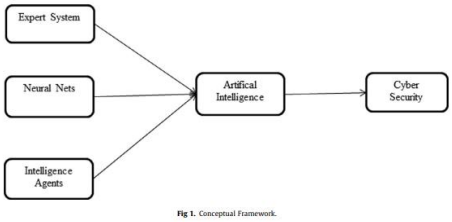

Fig 1. Conceptual Framework.

Source: Shamiulla, A. M. (2019). Role of artificial intelligence in cyber security.

II. DATA ANALYSIS AND INTERPRETATION:

A survey questionnaire was used based on Likert scale for reaching out to the desired respondents and was distributed among them by self-administering in case of any queries. 100 samples with the age ranging from 16 to 40, in general public were chosen and responses analyzed by applying simple Percentile analysis. The respondents filled the questionnaire as per their opinion and experiences. The responses of the samples are recorded below:

III. FINDINGS

The findings drawn out from the data analysis are as under:

Table 1: What are the impacts of cybercrime on the society?

S/N	Impacts	Response	Level of Agreement				
			SA	A	U	DA	SDA
1.	Child Pornography & Abuse	N	60	35	0	5	0
2.	Online Harassment	N	50	40	5	0	5
3.	Digital Piracy	N	35	60	5	0	0
4.	Hacking	N	40	40	5	10	5
5.	Intentional Defamation	N	30	40	20	5	5
6.	Spam	N	55	30	5	10	0
7.	Infringement of Copyright	N	45	25	15	15	10
8.	Monetary Loss	N	65	30	5	0	0
9.	Vulnerability Reports	N	60	30	5	5	0
10.	Denial of Services	N	45	30	15	5	5

Table 2: Why do computers play as tools for cybercrimes?

S/N	Reasons	Response	Level of Agreement				
			SA	A	U	DA	SDA
1.	Wide Availability	N	50	40	5	5	0
2.	Easy network access system	N	35	50	5	5	5
3.	Reasonably priced & Affordable	N	30	50	10	5	5

Table 3: What are the factors responsible for cybercrimes?

S/N	Factors	Response	Level of Agreement				
			SA	A	U	DA	SDA
1.	Growth of the Technology	N	45	35	0	10	10
2.	Economic factor	N	50	30	10	5	5
3.	Users' Negligence	N	60	30	5	5	0

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, January 2024

It is evident from **table 3** that majority of respondents 80% said that the growth of technology is one among factors that contribute to the existing of cybercrimes. Similarly, a sufficient majority of respondents 80% supported that economic is another factor.

IV. IMPLICATIONS (The future of AI-powered cybercrimes):

AI's potential impacts many countries and many companies that lead them to adopt the technology to improve business performance and enhance productivity and innovation.

AI seems to be a potential threat to humans in the forthcoming Gen – Zs.

Currently, there is no comprehensive law that governs AI in India. Proper legislative measures to be formulated to ethical standards.

The government's initiative of introducing biometric system Adhaar database affects general citizen's informational privacy which leads to Cyber Attacks/Threats. Strong education is required among the public to secure them from companies insisting Adhaar information for unauthorized purposes. This issue requires immediate redressal.

General Cyber Hygiene practices like Backup the data, Manage passwords wisely, Keeping the software updated, WIFI security (in public places), Using antivirus, Control physical access to data, Educate on data privacy policies, Avoid opening suspicious mails, etc. are mandatory for today's Cyber world.

V. CONCLUSION

With the advancement of technology and rapid globalisation, the personal and financial information of firms are stored on cloud and due to the increased dependence on digital technology, cyber-attacks have become common. Research Studies say that AI will accelerate the security defences against sophisticated cyber attackers. AI powered solutions can safeguard the data, monitor abnormalities in data access, quickly detect malicious activities and respond to security threats. AI offers many applications which we use in cyber security attacks.

REFERENCES

[1]. Sanyal, K., & Chakrabarti, R. (2020). Artificial Intelligence and India. Oxford University Press.

[2]. Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 19(12), 1462-1474.

[3]. Alhayani, B., Mohammed, H. J., Chaloob, I. Z., & Ahmed, J. S. (2021). Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings, 531.

[4]. S. Dilek, H. Çakır and M. Aydın,"Applications Of Artificial Intelligence Techniques To Combating Cyber Crimes: A Review", International Journal of Artificial Intelligence & Applications (IJAIA), vol. 6, no. 1, 2015.