AI: perilous threat to both physical and cyber world

Dr. Ajay Shriram Kushwaha
Associate Professor
School of Computer Application
Lovely Professional University, Punjab

Anmol K Sachan
Student Researcher
School of Computer Application
Lovely Professional University, Punjab.

Abstract *–Internet evolution during 80s brought technology and now AI becomes most dominating technology were lots of companies are being funded just because of their unique idea on AI few of big players in funding are OpenAI, GoogleAI etc.AI gains its popularity for solving multi-dimensional problems almost in every sector but as we know coin has its 2 sides another dark side of AI is getting indulge and programmed to carry on cyber-attacks with intention to never get caught by replicating into clusters to become undetectable, thus cyber criminals are using AI as a weapon. In this research article authors highlighted the impact of AI on both cyber and physical world and its consequences.*

Keywords *– AI, Artificial Intelligence, Cyber Security, Cyber Threat, Physical Threat, Cyber Criminal.*

I. Introduction

Critical attacks and massive breaches escalated dramatically and as per prediction by Appknox, “Year 2020 may reach $5 trillion costing related to damage caused by cybersecurity breaches [9]. For sure this decade will make humans evolve faster than in the past, in every field from the virtual world to the physical world. Cyber criminals[1] now-a-days are actually playing and thinking way beyond and differently than anyone else, a good example will be from **DEFCON 2017** conference, where a security company **Endgame**[2] revealed how it created customized malware using **Elon Musk’s OpenAI**[3] framework to create malware that security engines were unable to detect, Sounds scary but it's true [10].

AI already plays a major role everywhere and is therefore increasing threats for example:

- IT Companies might be compromised by losing control on their cyber physical devices which are responsible to routing of train management, traffic management or overflow safety of dam, etc.
- Fraud related to money, credit card fraud, online banking fraud.
- According to Deloitte and Forbes Insights, “Brand reputation as the highest strategic risk area for any company” which could be in danger due to AI penetration in business solutions.
- Communicable devices connected to IoT which are using AI and ML may cause intrusion or probable man-in-middle attacks.
- Safety and security of patient might occur interference in their medical devices or recommendation systems in a clinical setting [11].

II. Artificial Intelligence: Pros & Cons

AI has both the sides holding advantages and disadvantages related to security for both physical and cyber world we are hereby discussing few of them below.

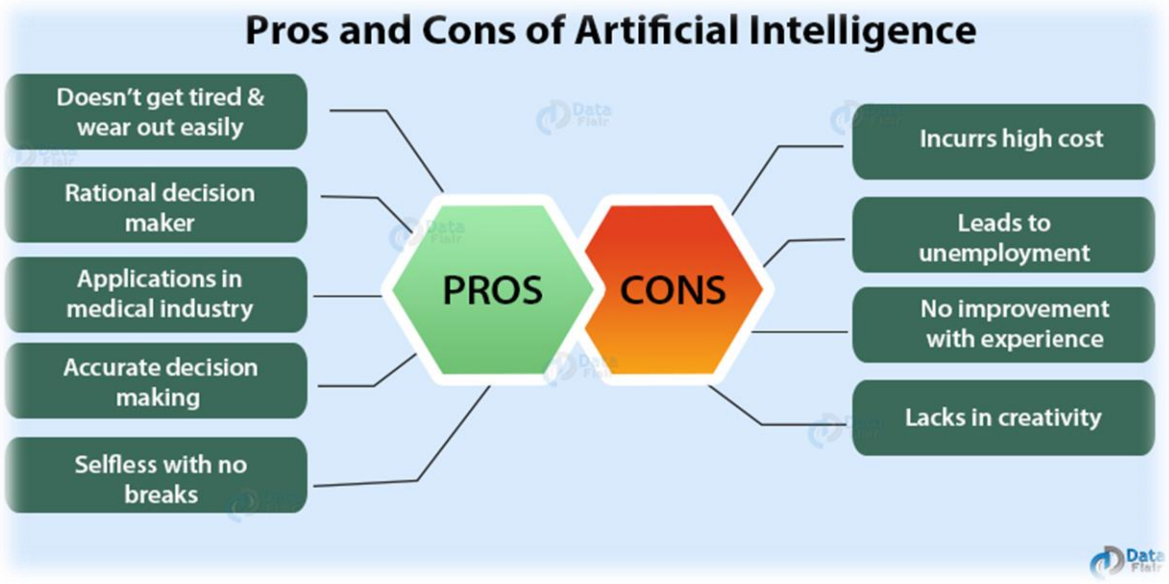

Fig.1 Advantages and Disadvantages of Artificial Intelligence [8]

❖ **Advantages of AI are given below**

1. Human makes to many errors but not machine thus AI will be helpful.
2. No tear and wear, tiredness to AI
3. AI assistance devices and programs helps human to solve their day-to-day chores
4. AI act as rational decision maker compared to human by taking right decisions.
5. AI programs is effective to repetitive jobs.
6. AI doing great in providing support for medical applications by assisting Doctor's in critical decision-making during operations
7. When it comes to human safety implementing AI helps to overcome life threating risks.

❖ **Disadvantages of AI are given below**

1. Implementing AI is costly affair and its complex machine plantation.
2. No matter how AI is helpful still it could not replicate human for many reasons in critical situation where situational decision required rather than logical.
3. AI still cannot be improved with experience thus it cannot cope up with dynamic environment and so they are unable to alter their responses to changing environments.
4. Machines could not be creating thus expecting creating through AI is not possible yet.
5. AI leads to unemployment which is riskiest and causing serious impact on human employment.

III. Smart and IoT based Botnets

Smart botnets, cluster-based attacks, Swarmbots, i.e., making them Intelligent by making them IoT Devices, making them communicate globally, Decide and launch a cluster-based yet more powerful attack, has been addressed by the Fortinet and other vendors often and is common too. These could make systems vulnerable at a Large scale at once. Each of the zombies become more Intelligent with local knowledge sharing, **WITHOUT A BOTNET**[4] instructing them and hence making an army of Zombies or simply a cyber weapon[5] that can be used to perform attacks like DDOS, Mining etc. well it's all on the creativity of the attacker.

These swarm technologies use hive nets which is an amazing concept, it allows the whole system to learn from its past behaviour and become more intelligent. Swarm Technology is said to be a collective behaviour of decentralized and self-organized systems, creating an IoT Botnet.

IV. Social Engineering / Phishing Attacks

AI can just change the whole game of how an attacker attacks the victim, just think of the possibility what if an attacker with the help of AI could create an autonomous system that can call, mail spoofing, text automatically may be use VOIP to do Vishing and by just using OSINT to create database and then just calling and pretending to be some relative or any bank employee asking the victim to pay money or update bank account or any attack that may cause to harm victim, and the worst part about this kind of system would be it will be untraceable if further ideas are included. The System could be trained to maintain the major acuteness to the Genuinity and to be convincing at the same time. In tests involving 90 users, the framework delivered a success rate varying between 30 and 60 per cent, a considerable improvement on manual spear phishing and bulk phishing results [6].

V. Threat to Physical World

Lots of devices in fact every third node on the internet is connected and is somehow being used, just think of the total shutdown of the internet by an AI? Is it possible well probably yes if its intelligent and powerful enough, but the question is who will be the person or what if due to just coincidence it could happen, a good example could be "Facebook AI bots[7] develop own language, start planning to murder us all" Alice and Bob, as the hell-bots were called, started off innocently enough (also: were not racist) – doing the robot banter, having a digital laugh and just genuinely being lovely, but later on they created their own language and started discussing evil, Facebook shut down the whole project, the question arises "What if, What if the things could go out of our control?"

Conclusion

Due to an extreme shortage of cybersecurity professionals, many companies are turning to AI to protect themselves from malicious attacks, and the worst thing could be what if AI System itself is hacked or somehow starts behaving maliciously, and the worst case scenario could be you never knew that it was compromised because eventually some cyber-attack will definitely be there may be it could have happened or it will be.

The tug of war between hacker and security team will go on with more advanced cyber weapons and defense methods, but the real test will be parsing through misinformation and false marketing claims of 'Artificial Intelligence' that isn't intelligent at all and finding the programs that work.

References-

1. Giovanni Bottazzi, Gianluigi Me, Chapter 17 - Responding to cybercrime and cyber terrorism—botnets an insidious threat, Editor(s): Babak Akhgar, Andrew Staniforth, Francesca Bosco, Cyber Crime and Cyber Terrorism Investigator's Handbook, Syngress, 2014, Pages 231-257, ISBN 9780128007433, https://doi.org/10.1016/B978-0-12-800743-3.00018-9.
2. EndGame, Inc. published by Wikipedia, URL https://en.wikipedia.org/wiki/Endgame,_Inc.
3. OpenAI, published by Wikipedia, URL https://en.wikipedia.org/wiki/OpenAI
4. Christopher C. Elisan, "Malware, Rootkits & Botnets A Beginner's Guide", 1st Edition, 2012, McGraw-Hill Education, Pages 386, ISBN 0071792066.
5. David E. Sanger, "The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age", 1st Edition, 19th June 2018, Crown, Pages 384, ISBN 9780451497895.
6. Dr. Erdal Ozkaya, "Learn Social Engineering", April 2018, Packt Publication, ISBN: 9781788837927.
7. Jordan Novet, " Facebook AI researcher slams 'irresponsible' reports about smart bot experiment", 1st August 2017 published by CNBC, URL https://www.cnbc.com/2017/08/01/facebook-ai-experiment-did-not-end-because-bots-invented-own-language.html

8. An article, "6 ways #hackers will use #machine #learning to #launch #attacks" published by National Cyber Security on dated 22nd January 2018 URL - https://nationalcybersecurity.com/6-ways-hackers-will-use-machine-learning-launch-attacks/.

9. Ryan Goosen, Et.al, "Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution" article published by BCG on dated 13th November 2018 URL- https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx.