International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 12 | Dec 2019 www.irjet.net p-ISSN: 2395-0072

Intervention of Artificial Intelligence in Cyber Security

K. Sindhu[1], D. Chaitanya[2]

[1]*Department of Cyber Security, Andhra Pradesh, India.*
[2]*SAS Analyst, Integra Technologies, California, USA.*

Abstract - Data has become the major aid in many of the organizations and securing the data from wrong hands is the main aim of cyber security experts. They go through a great scuffle to deal with the attacks as even a small loop hole in the network could cause the attackers to penetrate into the systems data ,which would down the organizations reputation and lead to its downfall. Using lots of rich data, Artificial intelligence involvement along with machine learning in Cyber security could minimal the cyber attacks. With the use of Artificial intelligence the process of securing data could me automated with a minimal or no human intervention. This paper depicts the use of Artificial intelligence in cyber security , how it defends the cyber attacks and protects the data from unauthorized users.

***Key Words*: Artificial Intelligence(AI), Machine Learning, Cyber security, Cyber attacks, automation, data sets.**

1. INTRODUCTION

With the progression of internet, the phase of crime has completely deviated. Cyber attacks have become more prevailing what we call as cyber crimes. Though cyber experts are coping-up with advanced technologies and methods to defend these crimes, still attackers are nearing with unique and unfamiliar virus codes to break the system security and penetrate into it unilaterally. It has become a perpetual process. So there is an immediate compulsion to enhance the security more and more to protect data from illegal approach.

Artificial intelligence is the trending technology being used by many organizations to safe-guard themselves from intruders. Dark trace, cylance like companies are already using advanced techniques to ensure high end security to the systems using Artificial Intelligence to provide security tools. With the use of AI for cyber security, cyber attacks can be detected even before they occur and could be defended at earliest as possible.

2. The approach to AI in Cyber Security

Cyber AI is the self learning technology like the human immune system. It learns from the data and activity that it scrutinize on the premises. This self learning ability empower cyber AI to divulge rare and formerly unnoticed patterns in cyber attacks. AI functioning is a mimic of human mind and it works on the basis of data sets that is already fed to it. Taking into count the previously happened cyber crimes, information on malware and the counter work done by the experts to defend them, all this data is collected and given as a historic data to AI in the knowledge base.

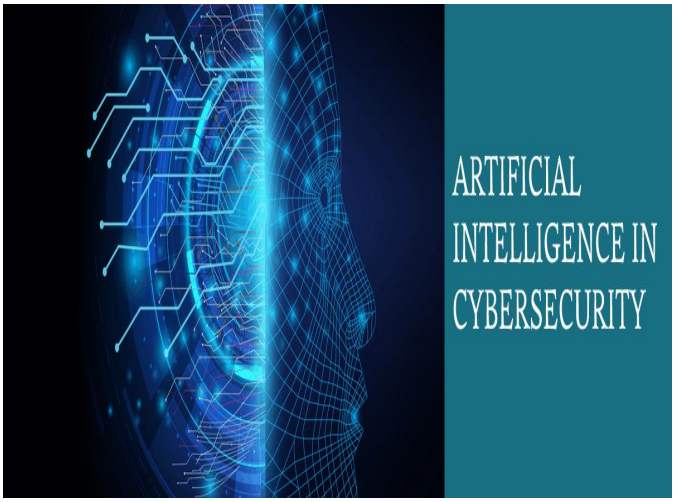

Fig-1. Artificial intelligence in Cyber Security

AI when it finds abnormal activities in the system it notifies an issue to the network admin on the dash board and finds for appropriate measures to defend the attacks by going through the data sets available in the knowledge base. If the attack is previously seen and the defend techniques for that attack is already stored in the data set AI acts the same like the information given in data sets to oppose the attacks. If the attack is new to AI it then implements machine learning. As like the human immune system that fights against the new bacteria, machine learning which is a sub-domain of Artificial intelligence, fights against new attacks that never been seen before. Machine learning has the ability to automatically learn and improve unsupervised data from supervised data. It uses mathematical and statistical ways to extract information from data and with that information machine learning tries to guess the unknown. Once the attack is prevented AI updates the knowledge base and searches for any new attacks and system abnormalities.

3. Algorithm

Step1:

Analyse the network traffic, system logs and user activities to see if there are any abnormal activities.

Step2:

If there are any system abnormalities find the defend mechanisms in the historic data.

Step3:

In case of already seen attack follow the same measures as per the data in knowledge base

Step4:

For new attacks use machine learning techniques to self defend the attacks.

Step5:

Once the attacks are detected and defended issue a notification on dashboard, update the knowledge base and check for new attacks and abnormalities.

Step6:

If the attacks couldn't be solved notify the network administrator on the dash board and check for new attacks and abnormalities.

4. Is AI a solution for Cyber security or it's another threat?

Artificial Intelligence if not used properly could definitely create a massive destruction. When proper and sufficient data is not given to the knowledge base false positives and false negatives could be happen which is again a hassle to the security experts. As everyone are running towards AI and machine learning, for most of the solutions they should be very careful while dealing the above mentioned subjects. When AI used by wrong hands, the same technology which secures the data can be a threat to data. Attackers can create advanced AI proof virus to hide the presence of attacks in the system. When these viruses are spread into system, even AI couldn't detect these attacks and these AI proof attacks could slowly penetrate into all the systems of the network causing to data theft, data manipulation or could also lead to ransomware.

In order to build and keep AI systems ready, companies need humongous amount of hardware and software supplies. AI has the equal advantages and disadvantages when used in Cyber Security. But when it is properly used it is a great boon for cyber security experts as it is a automated process i.e. once the proper and relevant data regarding attacks and its defense mechanisms is given, AI automatically monitors the system for any abnormalities and defends the attacks. AI could even detect any minor system changes which humans cant and works effectively and efficiently. As AI can give automated response it could work with no man power and also it consumes very less time to do its work saving the time, resources and cost.

4.1 Solutions to use AI effectively

A good AI solution requires lots of rich data and AI domain expertise's. Update the data sets thoroughly with the latest cyber risks and techniques to eradicate the attacks. Having cyber security teams testing the systems and networks for potential gaps and fixing them at the earliest could minimize the risk of cyber threat. Give loads and loads of information on how people do their works in investigating cyber attacks to AI. Track everything a human do with their consent and record every click they do, every website they go to every step they do in that journey of investigation. Capture all the data regarding how they find new attacks and the steps they take to find solutions to new attacks and feed this in data set. Replicate it in a machine learning platform to teach it how to respond to new attacks.. This is the data what ethical hackers do when they are investigating for attacks. Through this we can build systems that are very effective at replicating that process, taking the leads from weird things happening somewhere inside an organization and responding quickly to safeguard the systems data from black hackers. AI should be trained such that it has a potential of changing the permissions of the user according to the place of accessing data.

5. CONCLUSION

AI have potential to act much earlier than humans. Cyber AI's work well with machine learning to automatically detect and defend cyber crimes with minimal human intervention. The more data given to AI, the best effective results it produce. The working of AI is completely dependent on the data sets given to it. AI could also be used by attackers to develop AI proof attacks. To enhance security and safeguard the systems data against anomalies use firewalls and malware scanners to protect systems and constantly get updated to redesigned hardware and software's. Use data protection techniques like pseudonymization and data encryption. To get maximum good harvest from AI. It should be taken care by good cyber security farmers who have sound knowledge relating AI.

6. REFERENCES

[1] Alex Mathew "Cyber security and security automation", Advanced computing: An International Journal (ACIJ), vol.10, No.6, November 2019.

[2] Arockia panimalar.s, Giri Pai.U, Salman Khan.K, "Artificial intelligence techniques for Cyber security", International Research Journal Of Engineering and Technology (IRJET) vol.05, Issue: 03, March 2018.

[3] IBM. "Artificial Intelligence for smarter kind of Cyber Security" IBM, 16 August 2018, "https://www.ibm.com/security/artificial-intelligence"

[4] Aimee Laurence "The impact of Artificial Intelligence on cyber Security" August 22, 2019, "https://www.cpomagazine.com/cyber-security/the-impact-of-artificial-intelligence-on-cyber-security/"

[5] Vahakainu, Petri and Lehto,Martti. Artificial Intelligence in Cyber Security environment, Academic conferences International limited, Reading 2019.

[6] Siddiqui zeeshan, Yadav sonali, Hussain md., "Application of Artificial Intelligence in fight against Cyber Crimes: A review", International Journal of advanced Research in Computer Science, vol.9, No.2, pp. 118-121. 2018.

[7] Andrew Tsonchey "What will the impact of AI be on Cyber attacks", December 4, 2019. "https://www.youtube.com/watch?v=hUwBzCOEF14 "