International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

USE OF ARTIFICIAL INTELLIGENCE IN CYBER DEFENCE

Monica G. Tolani[1], Harsha G. Tolani[2]

[1]Information Technology Department, Thadomal Shahani Engineering College, Mumbai, India
[2]Computer Engineering Department, Vivekanand Education Society's Institute of Technology, Mumbai, India

---

Abstract - *Without substantial automation the speed of processes and the amount of data to be used cannot be decided by humans in protecting the cyber space. Thus, cyber security experts face a lot of encounters due to the outburst of IOT and linked devices in this digital world. The very common concern now is Cyber-attacks, which is very minded diverting. The related information can be hacked quickly, if a proper security system is not available. One of the most common causes for cyber-attacks is owed to the intruder. With the help of artificial intelligence and by enhancing the process of security intrusion is avoided at various levels of the layers in the network system. In order to prevent security breaches and attacks, the experts need help so that they can respond to the attacks. The successful resolution of cyber security problems with the help of solely strategies of the AI area unit has become obvious. Hence, for securing cyberspace, AI has become a transformative technology. This paper states the use of AI in cyber defense. This study will help the application to block the intruders who are trying to modify or access the data present.*

Keywords:- AI, cyber-attacks, cyber defense, IOT, intruder

INTRODUCTION

The incorporation of Artificial Intelligence into security systems can be used to reduce the ever increasing threats of cyber security that is being faced by the global businesses. As data collection, storage capabilities and computing power are increasing, the use of Machine learning as well as Artificial Intelligence (AI) is broadly being used across the industries.

As AI systems are able to efficiently learn from every cyber attack, they are used to protect the confidential data of organizations from cyber attacks. AI systems have an ability of detecting even small but important deviations from normal and so they are used as a key weapon for managing cyber attacks.AI systems perform the most crucial task in cyberspace security for intrusion detection and prevention. A vast security mechanism can be built with the help of cyber security and AI logic. The data and network can be protected from unauthorized access by cyber security, whereas AI aids the methods of machine learning with the ability to improve the access time of the system by learning from the data. AI can detect present and future threads which are yet to be discovered by using knowledge. The decision making in the human brain is limited in its capability to cope up with the different environment or to discover multiple variables of different kinds. So to prevent different attacks which are developing day by day, a proper kind of defense is necessary.

FORMS OF ARTIFICIAL INTELLIGENCE

In the past couple of years, Artificial intelligence has gained an incredible momentum. AI is a subdivision of computer science.AI aims at developing computers, which are proficient of performing activities that are considered 'intelligent' by humans. AI today can be divided into three basic and caliber categories:

1. Artificial Narrow Intelligence (ANI)

The most common AI is ANI which is narrowly focused on a single task, operating in a pre-defined range. It is a stream of intelligence which is eminent to perform a single task with smartness.ANI learns about a single task with smartness and then performs it proficiently. In many aspects of our daily lives, we can see this intelligence as the most common technology. This intelligence is found in smartphones like Cortana and Siri where it helps the users with their problems by responding to them when requested.

2. Artificial General Intelligence (AGI)

The AI that has the ability to think generally is AGI. AGI improves based on their past learnings and make decisions without previous exposure or experience. It is comparatively as intelligent as the human brain. It has the ability unlike ANI to learn and improve itself to perform various tasks. This category of artificial intelligence systems is known as 'Strong AI', since it works like humans. An example of AGI is Pillo robot which plays an important role in healthcare by answering the questions related to the health of the family. It gives proper guidance about their health and distribute the pills. Thus, this powerful technology is a necessity for living with a live-in full-time doctor.

3. Artificial Super Intelligence (ASI)

A set of intelligence which is more dominant and sophisticated than a human's intelligence is Artificial Super Intelligence. One of the most efficient and developmental forms of intelligence is Human's intelligence. Super intelligence can exceed this efficient human intelligence. Super intelligence has the power to think about abstractions which is not possible for humans to think. Thus, the power of humans to do things lies with this type of AI, it can even do more than these things. The first humanoid robot is Alpha 2 which is developed for the family. This robot has the ability of managing and operating the things of a house. It is a high-powered robot which can even notify about weather conditions.

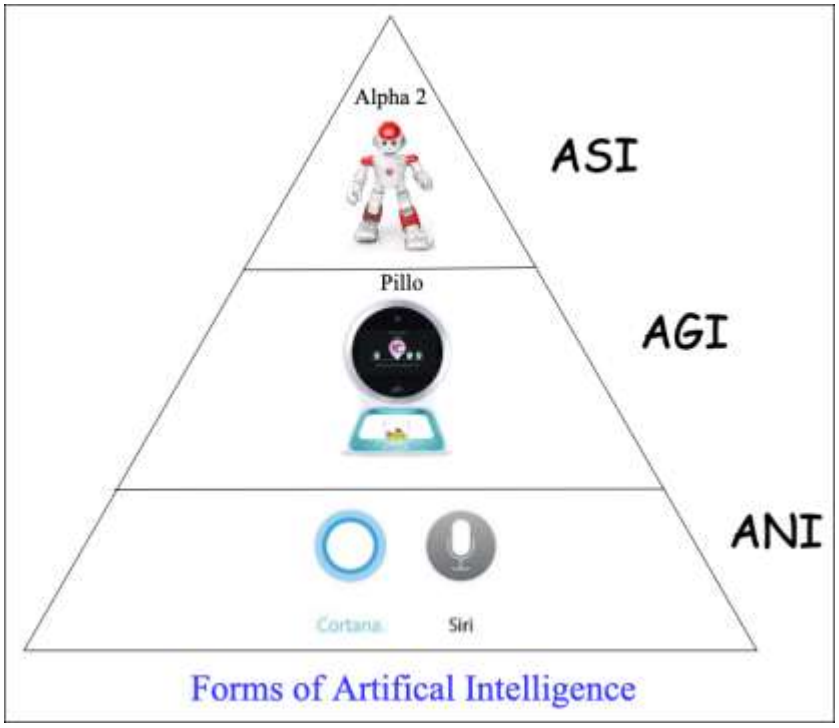

Fig 1. Forms of AI

WHAT ARTIFICIAL INTELLIGENCE IS TO CYBER DEFENCE

The traditional methods are failing to detect malware and cyber security threats. The organization's security firewalls are constantly being bypassed with new ways by the cyber criminals and thus giving a threat to an organization's security. The sole way to fight against hackers is to be more planned and smarter.

New security technologies with Artificial Intelligence programs are being found to detect extraordinary behavior on a network. The similarities and differences within a data set are being detected and reported for anomalies by AI which uses machine learning. Machine learning is a component of AI which helps in the recognition of the patterns and prediction of their effects based on past data and experience. In most cases, AI systems generate results that are related to human functioning

using machine learning technology. The downside of malware execution can be obstructed by using ML linked with application isolation which is also published in an article in Forbes titled 'Separating Fact from Fiction: The Role Of Artificial Intelligence In Cybersecurity'. It also states that the use of this isolation helps in eliminating the flaw so that no data is compromised and it prevents the malware from moving laterally into the network. The security experts are being facilitated by the AI techniques since it removes the noise or unwanted data by learning from the data and it even detects any anomalous activity by understanding cyber environment. The generation of cyber courses of action (COAs) on the detection of cyber threats with the help of automated techniques of AI benefits cyber security.

The existing detection and response capabilities of security system can be enhanced and new abilities can be enabled in preventative defense with the help of AI. The organizations apply AI at three levels to improve existing cyber security systems and practices.

a. Prevention and Protection:

The AI-enabled prevention and protection systems will benefit cyber security by using advanced machine learning techniques to harden defenses in the future. The humans can also interact flexibly with algorithmic decision making by using these systems.

b. Detection:

Some fundamental shifts are set up by AI. One shift is made to get methods that understand what baseline, or normal, network and system activity look like, so signature-based detection (it has a set of static rules relying on the updation and recognition of the attack signature) is transformed to more flexible and continuously improving methods. Any changes that appear abnormal are detected by AI algorithms without the need of an advance definition of abnormal. Another shift is to move beyond classic approaches based on machine learning that require large, curated training datasets. The recognition of sources of potential threats can be found using AI from internal and external sensors or small pieces of monitoring software. This monitoring software performs deep packet inspection by evaluating digital traffic.

c. Response:

The workload for cybersecurity analysts can be reduced using AI which helps prioritize the risk areas for attention. AI can also help them to intelligently transform their manual tasks(such as searching through log files for signs of compromises) to automated tasks, thus redirecting human efforts toward higher-value activities. Based on shared knowledge and learning, AI can also facilitate intelligent responses to attacks, either outside or inside the perimeter.

For example, today we are using the technology to deploy semi autonomous, intelligent allurements or "traps" that are used to create a duplicate of the environment which are being penetrated by the attacker and make them believe that they are on the intended path and then use deceit to identify the culprit. The networks can be segregated dynamically into isolated valuable assets in safe places using AI-enabled response systems. These systems, even help to redirect attackers away from vulnerabilities or valuable data. Thus, these systems help in increasing the proficiency of the analysts by not spending time on finding them and focus on investigating high-probability signals.

Currently, fields like healthcare, manufacturing, education and cyber security are already flourishing with AI. In today's digital world Cyber security is the main concern, there are still problems about the impact of AI. A complete error-free cyber-security services are being assured with AI, since it is totally machine language driven.

CONCLUSIONS

Billions of transactions are being processed per day by organizations nowadays. This huge volume of data is being targeted by cyber attackers and it becomes impossible to manually check for intrusion. To ensure cyberspace security, real time and proactive detection of these intrusions is needed. AI systems are able to identify the cyber attacks by differentiating benign and malicious activities in computer networks. A constant monitoring and reporting of an organization's network is performed by AI systems which makes incident response faster. The in-progress cyber attacks can be prevented as well as can be stopped by this AI systems. AI systems have the ability to understand different patterns by performing deep analysis of network's

behavior and make self-healing networks by adapting to new situations by thousands of learning iterations. Due to the huge capabilities, a significant role to combat cyber- attacks is being anticipated by artificial intelligence.

Thus, Intelligent Security System is needed in the Current scenario forthcoming development in malware and cyber-attacks. AI techniques are more robust and flexible contrasted with Contemporary cyber security solutions. Thus, in this growing number of advanced cyber threats AI techniques help in increasing security execution and provide better defend system. As organizations are witnessing rising incidence of cyber-crimes so there is a need for fast growth of artificial intelligence in the cyber security market.

REFERENCES

1. Enn Tyugu,"Artificial Intelligence in Cyber Defense", 3rd International Conference on Cyber Conflict, 2011.
2. Harini M Rajan, Dharani S, "Artificial Intelligence in Cyber Security - An Investigation", International Research Journal of Computer Science (IRJCS), Issue 09, Volume 4, September 2017.
3. Priti Bali, "Artificial Intelligence: A Boon or Threat for Cyberspace Security", International Journal of Engineering, Science and Mathematics, Vol. 7,Issue 4, April 2018,
4. A. Anitha, Girish Paul, Savera Kumari,"Cyber Defense Using Artificial Intelligence", International Journal of Pharmacy and Technology,2016.
5. Arockia Panimalar.S, Giri Pai.U, Salman Khan.K, "Artificial Intelligence Techniques for Cyber Security", International Research Journal of Engineering and Technology (IRJET), Volume: 05, Issue: 03, Mar-2018.
6. Yallamanda Reddy, A. Thirupathaiah, "Artificial Intelligence in Cyber Defense", International Journal of Advanced Trends in Computer Science and Engineering, Vol.3, October 2014.
7. Dr. Sunil Bhutada, Preeti Bhutada,"Applications of Artificial Intelligence in Cyber Security", International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), Vol 5, Issue 4, April 2018.
8. Amaan Anwar & Syed Imtiyaz Hassan, "Applying Artificial Intelligence Techniques to Prevent Cyber Assaults", International Journal of Computational Intelligence Research, Volume 13, Number 5 (2017).
9. Priti Bali, "Artificial Intelligence: A Boon or Threat for Cyberspace Security", International Journal of Engineering, Science and Mathematics Vol. 7, Issue 4, April2018.