International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

A Futuristic Approach: Incorporating Artificial Intelligence with Cyber Security

Shefali Nangia[1], Megha Malik[2], Deepak Chahal[3], Latika Kharb[4]
[1,2]*MCA Student, Department of IT, Jagan Institute of Management Studies, Delhi, India*
[3,4]*Professor, Department of IT, Jagan Institute of Management Studies, Delhi, India*

***Abstract*: In a digital world of IoT and inter-connected devices, cyber security is becoming reason of concern. The experts need all the help to prevent attacks and security cracks and respond to the attacks.**

As it can be seen, that is not possible to create a hard-wired logics-based software system to handle such severe cyber-attacks. And it has been seen from quite a time period, that if procedures of Artificial Intelligence are implemented nicely, numerous cyber securities can be settled with progress.

This article talks about Artificial Intelligence that can be referred to as the ability of a machine or a computer program to think and learn. The concept of AI is based on the idea of building machines capable of thinking, acting, and learning like humans.

And Cyber Security, which simply refers the techniques of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

As the number of cyber-attacks is increasing, Cyber security is becoming a major concern. So, here we have talked how Artificial Intelligence can help in this, various AI techniques that can be implemented to Cyber Security and what is the future for the same.

***Keywords*: Artificial Intelligence, Cyber Security**

1. Introduction

A. What is Artificial Intelligence?

"Artificial intelligence (AI) in simple terms refers to an area of computer science that emphasizes on the creation of intelligent machines that work and react like humans." [1]

In RFID Journal, 2009 edition, Kevin Ashton stated that "In the real world, things matter more than the ideas".

Imagine what if we had computers that knew everything we need to know about the things around us - without human help - and this would eventually reduce waste, loss, and cost. And hence, we would know when and where our things need replacement, repairing, etc. And this is possible only with the help of IoT (Internet of Things) and AI.

Ideas and information do matter, but not more than the things around which they evolve.

And perhaps, we can say that IoT Won't Work Without Artificial Intelligence.

And some activities that such devices (or machines) are designed for are: Speech recognition, learning, problem solving and many more.

Now, coming to Cybersecurity. Cybersecurity, also known as computer security or IT security, can be referred to as the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide [2].

2. The emergence of AI in cyber security

AI is by no means is a pure solution to cyber security. It needs human interaction and training in AI-speak to continue to learn and improve, correcting for false positives and cybercriminal innovations. [3]

All the upcoming of cyber security products are trying to incorporate Artificial Intelligence (AI) and Machine Learning (ML) technologies with their products so as the developers can detect and block abnormal behavior, even if it does not exhibit a known "signature" or pattern.

This way the machine takes away this burden of the personnel of spending time on such repetitive and tedious tasks, thereby allowing them to focus on some more challenging tasks of finding new and complex threats.

3. Emerging role of artificial intelligence in cyber security

In early days Computer Security and AI were not connected to each other.

Artificial Intelligence focused mainly on reducing human work load whereas Security personnel used to ensure as secure as possible transmission of data.

But, as now and how Cyber-attacks are increasing and targeting to simulate the genuine performances, Cyber security is a getting a major concern.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a very good example of connection of artificial intelligence and security.

It is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot.

For example, humans can read distorted text as the one shown below, but current computer programs can't.

This term CAPTCHA was originally coined in year 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University.

And as per these three, "any program that passes the tests generated by a CAPTCHA can be used to solve a hard-unsolved AI problem."

They argue that the advantages of using hard AI problems as a means for security are twofold. Either the problem goes unsolved and there remains a reliable method for distinguishing humans from computers, or the problem is solved and a difficult AI problem is resolved along with it. In the case of image and text based CAPTCHAs, if an AI were capable of accurately completing the task without exploiting flaws in a particular CAPTCHA design, then it would have solved the problem of developing an AI that is capable of complex object recognition in scenes.

Practicing Artificial Intelligence and its several techniques can be useful in detect any type of interferences and responding to anonymous before spreading itself.

Artificial Intelligence systems that are intended to learn and adapt, and are capable of identifying minutest of the changes and acting to it much earlier than humans would.

And as the number and intensity of cyber-attacks are growing these days, in form of sophisticated malware and cyber terrorism-researchers and security experts are more desperately looking for new and better ways to address these kinds of cyber-attacks and threats.

And definitely, the old traditional techniques and tools like firewalls and Data Loss Prevention (DLP) are going all in vain now.

To this, Bruce Daley, Principal Analyst at technology research and consulting firm, Tractica and the author of "Where Data Is Wealth" (Play Technologies, 2015) had to say that, "We have entered a different era. As society digitizes everything of value, we create irresistible targets for people who want to engage in criminal activities"

Whereas today, he says, "We're seeing a level of ingenuity and sophistication from criminals that places even the most modern and sophisticated IT systems at risk."

Which surely is leaving us more concerned now.

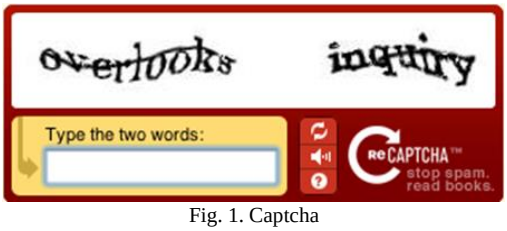

Fig. 1. Captcha

4. Techniques for implementing artificial intelligence (AI) cyber security

There are different approaches to using AI for cyber security. The very step to it is to determine what is appropriate for the organization and what not.

Some software applications analyze raw network data to spot an irregularity, while others focus on user/asset/entity behavior to detect patterns that deviate from normal. The types of data streams, how they are collected, and the level of effort needed by analysts all vary by approach.

The various techniques are:

A. Expert system

An Expert System refers to a computer system that copies the decision-making ability that of a human. A Knowledge-based can be best suitable example of an Expert System. Now, an Expert System comprises of two main parts:

1. The Knowledge Base, which represents the descriptions and assertions in the real world.
2. The Inference Engine, which is an automatic reasoning system. It is estimating the current situation of the knowledge base.
3. CSIA (Cyber Security Artificial Intelligence Expert System)
   - CSIA (Cyber Security Artificial Intelligence Expert System) is one such expert system that comprises of both these above components [6].
   - Experts System also includes the Security Expert System.

A system which follows a set of rules to battle several kinds of cyber-attacks. With the help of Knowledge Base, it checks all the processes, if one is a good known process, then the Security expert system ignores it, else this system would terminate the process after that it is using the inference engine algorithms (rule sets).

Table 1
Components of an expert system

Components of Expert Systems	
Knowledge Base	Malicious IP Address
	Known Malware
	Known Virus
	Approved Applications
	Approved IP Addresses
	End Point Usage Statistics
Inference Engine	IP Address Geographical Location
	Connection Attempts
	Connection Patterns
	Frequency of Program Use
	Document Usage
	Login Timestamps
	Login Attempts
	Port Communication
	File/Folder Access Patterns

B. Neural nets

Neural Nets, also known as the Deep Learning. Neural Nets is a kind of advancement of AI.

Also, it is inspired by how our human brain acts and works in certain situations, which makes it more capable of learning any type of data.

In 1957, Frank Rosenblatt created an artificial neuron (Perceptron) which paved the way for neural networks.

Perceptron learn on their own and also identify the entity. They identify these entities on which they are trained by learning and processing the high-level raw data.

When we apply this deep learning to cyber security, we make a system capable to identify whether a file is malicious or legitimate or not, that too without any human interference.

Resulting in early detection of malicious threats, as compared to the only machine learning systems, these systems produce better results.

Neural Nets hence permits the exact detection of new malware threats.

C. Intelligent agents

Intelligent Agents (IA) is an autonomous entity which observes movements through sensors and acts upon an environment using actuators (i.e., an agent). They also use Knowledge Base sometimes to achieve their goals. They might be extremely simple or very complex. A reflex machine, for example, Thermostat is an intelligent agent, or Programs running in self-driving cars. These programs need to take "rational' decisions. Intelligent Agents are also created in showdown against Distributed Denial of Service (DDoS) attacks. In any case if there is a legal or business issue, it should be manageable to develop a "Cyber Police". Cyber police should have mobile intelligent agents.

5. Advantages of using AI techniques

From our above section, we learned about three AI techniques and their advantages, as and when implemented, can be as follows:

A. Expert system

- Decision making ability
- Knowledge Base
- Inference Engine
- Early intrusion detection

B. Neural nets

- Early intrusion and prevention
- DDoS Detection
- High Speed of operation

C. Intelligent agents

- Protection against DDoS
- Mobility
- Proactive

6. Future enhancement

When we use AI, there are various ways for the benefit of cyber security. In future, we may have most intelligent systems. The attackers or intruders will also use the AI for attacks.

Automated transportation will become a common thing in the future. In future, humans will be able to augment themselves with robots.

The future application of AI in cyber security, it will ensure in curbing hackers. The future of Machine Learning and AI is very bright.

7. Conclusion

The process of building applications has been a journey and it varies depending on one's application requirements and purpose [7]. In the current scenario, increasing development in threats and cyber-attacks and cyber security system is essential. Artificial Intelligence (AI) are more flexible and more powerful than the cyber security solutions. Therefore, it is increasing the security implementation and better defend system from a growing number of advanced and complex cyber threats. In which we have many benefits when we use the artificial intelligence techniques for cyber security. For AI techniques, we need human communication and training continuously.

References

[1] https://www.techopedia.com/definition/190/artificial-intelligence-ai
[2] https://en.wikipedia.org/wiki/Computer_security
[3] https://www.information-age.com/role-ai-cyber-security-123465795/
[4] Kharb, L. The Hackers: Shadow Brokers, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2017.
[5] https://en.wikipedia.org/wiki/CAPTCHA
[6] Arockia P Set al: Artificial Intelligence Techniques for Cyber Security, International Research Journal of Engineering and Technology, 2018.
[7] Kharb, L. A Perspective View on Commercialization of Cognitive Computing. In 2018 8th International Conference on Cloud Computing, Data Science & Engineering, IEEE.