Infopercept

Artificial Intelligence is the future of cyber security

Definition

- The theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages.

- Artificial intelligence is a science field that is interested in finding solutions to complex problems like humans do. Deep learning is a subdomain of machine learning and tries to learn the data with artificial neural network approach.

Abstract

- In this digital world, cyber security experts face a lot of encounters. The number of attached workplaces lead to heavy traffic, more security attack vectors, security breaches and lot more that the cyber area cannot be handled by humans.

- It has turned out to be evident that numerous cyber security issues are additionally settled with progress only procedures of Artificial Intelligence area unit acquiring utilized. Cyber security computing applications and analyses the views of improving the cyber security abilities by suggesting AI applications and the already existing methods

Keywords

- Artificial Intelligence
- Intelligent Agents
- Cyber Security
- Neural Nets
- Expert Systems

VIEW MORE

Introduction

The day to day raising and progressing cyber security threat facing global businesses can be reduced by the integration of Artificial Intelligence into cyber security systems. With AI, that peak of data could be carved down in fraction of time, which helps the enterprise to identify and recover from the security threat.

ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

- CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a very good example of connection of artificial intelligence and security. This requires end-user to insert the letters of some unfair image, on some occasions with the addition of a masked sequence of letters or digits that appears on the screen. Improvements in automatic character recognition software, which can be considered to be a reasonable advance in AI technology.

- Artificial Intelligence helps us in quickly identifying and analyzing new exploits and weaknesses to help ease further attacks and is an integral part of our solutions.

- Intelligence systems that are intended to learn and adapt, and are proficient of identifying even the minutes of changes in the settings, have the potential to act much earlier and based on vast trove of data than humans when it comes to analyzing novel types of cyber-attacks.

ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY

- Expert Systems - An Expert System is a computer system that copies the decision making ability of a human. This is a best example of Knowledge based system. It is composed of two sub-systems: the Knowledge Base and the Inference Engine. The knowledge base represents the illustrations and assertions in the real world. The Inference Engine is an automatic reasoning system.

- Neural Nets - Neural Nets is also known as deep learning. It is an advanced branch of AI. It is inspired by the functions and working of the human brain. Our brain has several neurons, which are largely general purpose and domain-independent. When we apply this deep learning to cyber security, the system can identify whether a file is malicious or legitimate without human interference. This technique yields a strong result in detecting the malicious threats.

- Intelligent Agents - Intelligent Agent is an independent entity which recognizes movement through sensors and follows up on an environment using actuators (an agent) and directs its activity towards accomplishing objectives. A reflex machine, for example, thermostat is an intelligent agent. It has the behavior like understanding agent interaction language, pro-activeness and reactivity. Intelligent agent is created in showdown against Distributed Denial of Service (DDoS) attacks.

ADVANTAGES OF AI TECHNIQUES

Expert Systems - Decision Support

- Intrusion Detection
- Knowledge Base
- Inference Engine

Neural Nets - Intrusion Detection and Prevention System

- High speed of operation
- DoS Detection
- Forensic Investigation

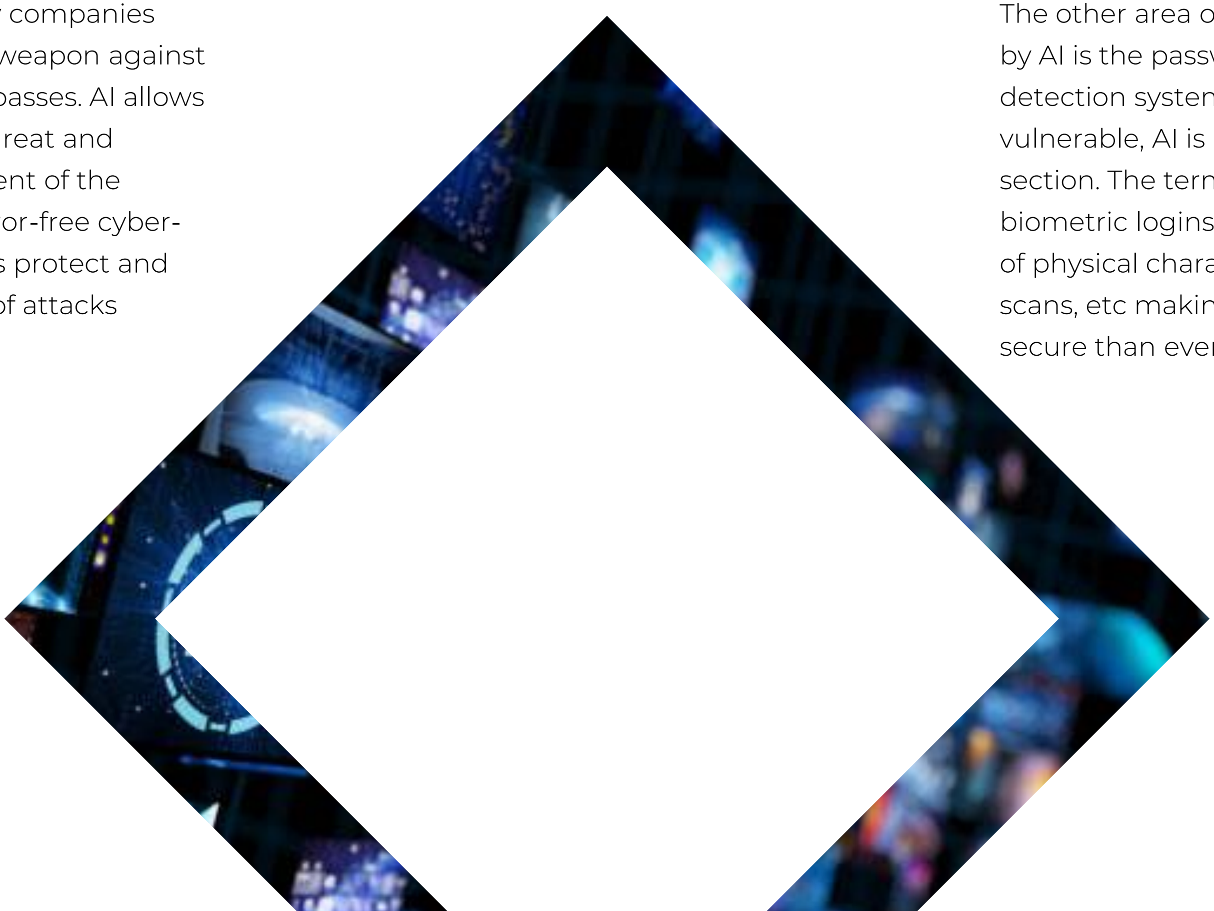
Intelligent Agents - Proactive

- Agent Communication Language
- Reactive
- Mobility
- Protection against DDoS

Infopercept

The Effect of AI in Cyber Security- The Positive Side

With the advancements in AI, many companies have started to use it as a powerful weapon against the puissant cyber attacks and trespasses. AI allows you to automate the detection of threat and combat even without the involvement of the humans it assures you complete error-free cyber-security services.AI let the defenders protect and stay strong even against the series of attacks such as virus and malware attacks.



The other area of cybersecurity that can be affected by AI is the password protection and authenticity detection systems. Since passwords are much vulnerable, AI is implemented a lot over this section. The term for such security systems is biometric logins. AI is being used for the detection of physical characteristics like fingerprints,retina scans, etc making the system more safe and secure than ever.

Other Side of AI- The Wrong One

The black hat people have also started to explore for how AI can be a solution for them as well. That means that the people with the wrong intentions have also started to gain authority over AI, making them more powerful and skilled to get their things done. They have started to develop the hacks and methodologies in order to break against the cyber securities.

Although companies have specific cybersecurity cells still the sophisticated attackers somehow find their ways towards breaking the breaches.

Conclusion

Artificial Intelligence techniques are more flexible and robust than contemporary cyber security solutions.As AI is adding values to the security sectors of the corporations and individuals as well, it is also spreading more power in the wrong hands. In order to give AI more authority in the near future for the security purposes, we need to stay sure that it stays with the white hat people only.

FUTURE ENHANCEMENT

We can use AI in various ways for the benefit of cyber security. In future we may have most intelligent systems than these techniques. Even the attackers or intruders will also use the AI for attacks. Clearly, the emerging advances in data understanding, handling and illustration what is more in machine learning will greatly enhance the cyber security capability of systems that would use them.

THANK YOU

For More Information Please Visit our Website

www.infopercept.com