www.ijrream.in Impact Factor: 2.9463

INTERNATIONAL JOURNAL OF RESEARCH REVIEW IN ENGINEERING AND MANAGEMENT (IJRREM)

Security Defenses in Artificial Intelligence Using Cyber Defensive Reasoning

[1]Mrs. M. Angelin Rosy, [2]Dr. M. Felix Xavier Muthu

[1]Assistant Professor, [2]Associate Professor

[1]Department of MCA, Er. Perumal Manimekalai College of Engineering, Hosur

[2]Department of Mechanical Engineering, St. Xavier's Catholic College of Engineering, Nagercoil

ABSTRACT:

The fast processes and the large of data to be used in defending the cyber space cannot be handled by humans without considerable automation. However, it is tough to develop software with hard-wired reasoning conducted on decision making level for efficiency defending against the dynamically evolving attacks in networks. This situation can be handled by implementing methods of artificial intelligence that provide flexibility and learning capability to software. This research paper represents a brief examine of artificial intelligence applications in cyber defense (CD), and study the possibilities of further improve the quality of value the cyber defense the power by means of become the intelligence of the defense systems. After studying the papers available about artificial intelligence approaches in CD, we can arrive at a judgment that useful applications already exist. It has become decided that many CD problems can be solved successfully only when methods of artificial intelligence are being used. Like, universal knowledge usage is necessary in decision making, and intelligent decision support is unsolved problems in CD.

KEYWORDS: *Artificial intelligence, Cyber security, Cyber security defense tools, Intelligent Cyber Defense techniques, Defense security service, System in cyber defense.*

1. INTRODUCTION:

Artificial intelligence in cyber security solutions rely heavily on algorithms of available data and these chunks of data are largely inputted by humans. As such, human intelligence is required in understanding the threat landscape before AI solutions kick in to detect cyber criminals and reduce damage. Many believe that AI is already being deployed for malicious purposes by highly motivated and sophisticated attackers. It's not at all

surprising given the fact that AI systems make an adversary's job much easier. Analyzing large data sets helps attackers designate their action based on online behavior and calculated money. Relating to models can go further and calculations the qualities to pay the sum of money demanded based on historical data, and even alter the size of pay-out to enlarge the chances and, therefore, earnings for cyber criminals.

2. ARTIFICIAL INTELLIGENCE:

Artificial intelligence the simulation of human intelligence in machines that are programmed to think like humans and imitate their actions. The term may also be applied to associate with a human mind such as learning and problem-solving. The ideal characteristic of artificial intelligence is its ability to justify and take actions that have the best chance of a desired objective a specific goal.

Artificial intelligence is based on the concept that human intelligence can be defined in a way that devices can easily achieve tasks, from the most simple to those that are even most complicated way. The goals of artificial intelligence include learning, reasoning, and the way in which something is regarded. As technology advances, previous a standard that defined artificial intelligence become out of date. Like, devices that calculate basic functions through best character something are no maximum considered to artificial intelligence, until now this function is now taken for granted as computer function.AI is continuously evolving to benefit many different organizations. Machines are wired using a cross-concerning approach based in mathematics, computer science, psychology, and more.

3. CYBER SECURITY:

Cyber security is techniques for protecting computers, networks, programs and data from not permitted access are aimed for exploitation. Network security includes activities to care for the usability, consistency, reliability and security of the network. Cyber security protects the data and reliability of compute the resources involving to an organization network. Its purpose is to look after those resources against all threat actors throughout the entire life cycle of a cyber-attack.

4. CYBER SECURITY DEFENSE TOOLS:

- Firewall. ...
- Antivirus Software. ...
- PKI Services. ...
- Managed Detection Services. ...
- Penetration Testing. ...
- Staff Training.

Firewall:

A firewall is a structure considered to check unofficial way from a private network. You can implement a firewall in a combination of hardware and software. Firewalls prevent unofficial internet users from access private networks connected to the internet, especially intranets.

Example:

A computer connected to a router has an address given to it by the router, while the router uses its own, single IP address to direct traffic.

Antivirus Software:

Antivirus software, originally designed to detect and remove viruses from computers, can also protect against a wide variety of threats, including other types of malicious software, such as key loggers, browser hijackers, Trojan horses, worms, root kits, spyware, adware, botnets and ransom ware.

PKI Services:

The Public key infrastructure (PKI) is located to both the combination of software, hardware policy, process, and actions necessary to create, manage, share out, use, store, and cancel digital certificates and public-keys. PKI-enabled systems provide strong certification and encryption of data by using cryptographic function. Unlike traditional identity processes where users are identified by passwords, a PKI issues a certificate via known, trusted channels and binds the certificate to a cryptographic key pair.

Managed Detection Services:

Managed detection and response (MDR) is an outsourced service that provides organization with risk hunt services and respond to pressure once they are exposed. Managed Detection and Response (MDR) is a managed cyber security service that detects intrusions, malware, and malicious activity in your network and assists in responding quickly to eliminate and mitigate those threats.

Penetration Testing:

Penetration is testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing is capable of computerized with software applications or performed automatically.

Staff Training:

- Learn about email security.
- Learn about social engineering and over sharing.
- Learn about passwords.
- Learn safe and secure file sharing.
- Learn how to surf safely.
- Learn how be safe in coffee shops.
- Safe Wi-Fi.
- Learn mobiles and smart devices security.
- Learn how to surf safely at home.
- Help your organization build a culture of information security awareness.

5. INTELLIGENT CYBER DEFENSE TECHNIQUES:

- SQL Injection Attacks (SQLi).
- Cross-Site Scripting (XSS).
- Man-in-the-Middle (MITM) Attacks.
- Malware Attacks.
- Denial-of-Service Attacks.

SQL Injection Attacks (SQLi):

SQL injection is one of the more dangerous and well-known, fail to interpret, security unprotected on the Internet, largely because there is no central may be stored of information available. The agreement resource for understanding, finding, make full use of and derive benefit from , and danger against this increasingly popular and particularly destructive type of Internet-based attack.

Cross Site Scripting (XSS):

Stored unrelieved XSS, which is when malicious virus script is injected directly into the unprotected application, and throw back XSS, which involves 'reflecting' malicious script into a link on a paper, which will activate the armed force once the link has been pressed.

Man-in-the-Middle Attacks (MITM):

Man-in-the-middle attacks are a common type of cyber security attacks that allows attackers to secretly listen to a conversation on the communication between two aims. The attack takes place in between two in a way that conforms to the law or to rules communicating hosts, allowing the attacker to "listen" to a conversation they should normally not be able to listen.

Malware Attacks:

A malware attack is a type of cyber attack in which malicious software performs activities on the actions computer system, usually without his/her knowledge. Nowadays, people use words like virus, spyware, and a sum of money demanded a lot of the word "virus".

Denial-of-Service-Attacks:

A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent justification users from accessing the service. In a DoS attack, the attacker usually sends desirable messages asking the server to validated requests that have invalid return addresses.

Defense Security Service:

The Defense Security Service (DSS) is a relating to security agency of the United States Department of Defense .Within areas of DOD responsibility, DSS is tasked with make easy personnel security researches, administer industrial security, and enact security education and knowledge training. A decision support system (DSS) is a supplied information system used to support decision-making in an organization. A DSS lets users sift through and study large amounts of data, and compile information that can be used to solve problems and make better decisions.

6. MACHINE LEARNING:

Machine learning is an function of artificial intelligence (AI) that provide system the capability to manually learn and get better from experience without being clearly programmed. Machine learning focuses on the growth of computer program that can access data and use it learn for themselves. Machine learning is a division of AI. With the purpose of all machine learning count as AI, but not all AI counts as machine learning. For example, representative reason – policy engines, expert systems and knowledge graphs – can be describe as AI, and no one of them are machine learning.

Artificial Intelligence in Business Management:

Artificial intelligence is defined as the assumption and increase of computer systems competent to execute responsibilities normally require human intelligence, such as image observation, communication appreciation, decision-making, and translation between languages. Artificial intelligence can be used to solve problems crossways the board. AI can help businesses increase sales, identify fraud, improve customer experience, automate work processes and provide analytical study. Logistics companies can use AI for better register and delivery management.

Example:

Artificial intelligence in business management voice to text features. Smart personal assistants, such as Siri, Cortana and Google Now. Automated responders and online customer support. Process automation.

Important Application of Artificial Intelligence in Bussiness:

- Machine learning,
- Deep learning,
- Robotics,
- Computer vision,
- Cognitive computing,
- Artificial general intelligence,
- Natural language processing and
- Knowledge reasoning is just some of the main branches of artificial intelligence.

Who uses Artificial Intelligence?

Artificial Intelligence is methods where machine, in exacting computer systems are caused by particular action to process like human intelligence, i.e., machines are add in place of humans. The various AI processes contain way of thinking, knowledge and self-correction.

Best Examples:

Best examples are Apple's Siri, Google's Allo.

Expert System in Cyber Defense:

Expert systems are the most widely used AI tools. An expert system is software for finding answers to questions in some application domain presented by a user. There is a great variety of expert systems from small technical systems to very large technical systems for solving complex problems. Conceptually, an expert system includes a knowledge base, where expert Knowledge about a specific application domain is stored. Besides the knowledge base, it includes an inference engine for deriving answers based on this knowledge and, possibly, additional knowledge about a situation. There are many tools for developing expert systems. Expert systems can have extra functionality for making calculations etc. There are more than varieties of knowledge description forms in expert systems; the most average is a rule-based description.

7. CONCLUSION:

Cyber-attack is one of the biggest threats to businesses, governments, and institutions today. More than 200 million personal records were exposed in data an act of breaking in 2016; including high-profile an act of breaking at the Department of Homeland Security and the Federal Bureau of Investigation (FBI).99 percent of utilize unprotected are already known. There is no lack of conviction that artificial intelligence is without and smart and faster than human, but it need human connect to get going. As the online industry is assuming complete online transparency not done of malicious cyber-attack is secure. So businesses need to focus largely on recruit and training AI experts who can work with the machine for product safety. Substance of the human brain and AI will certainly help in challenge against the techie.

References:

1. E. Tyugu. Algorithms and Architectures of Artificial Intelligence.IOS Press. 2007.
2. https://business.f-secure.com/whats-the-deal-withartificiai-intelligence-in-cyber-security.
3. (George, January 11, 2017) http://www.securityweek.com/role-artificial-intelligence-cyber-security.
4. Crosby, S. (2017, August 21). Separating fact from fiction: The Role of Artificial Intelligence in Cyber security. Retrieved March 16, 2018.
5. K. Trieu, and Y. Yang. Artificial Intelligence-Based Password Brute Force Attacks, 2018.
6. http://en.wikipedia.org/wiki/Expert_system.accomplished System. Wikipedia.
7. Machine Learning Techniques Applied to Cyber Security. (2017, September 10). Retrieved March 18, 2018, from https://towardsdatascience.com/machine-learning-techniques-applied-to-cyber-security-d58a8995b7d7
8. Marty, R. (2018, January 01). AI and Machine Learning in Cyber Security – Towards Data Science. Retrieved March 16, 2018, from https://towardsdatascience.com/ai-and-machine-learning-in-cyber-security-d6fbee480af0