International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY

Arockia Panimalar.S[1], Giri Pai.U[2], Salman Khan.K[3]

[1]Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu
[2,3] III M.Sc SS, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu

---

Abstract: *In this digital world, the outburst of IOT and linked devices, cyber security experts face a lot of encounters. The experts need all the help to prevent attacks and security cracks and respond to the attacks. 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 while not sizeable automation. Be that as it may, it is hard to create software system with standard mounted algorithms (hard-wired logic on deciding level) for successfully cautious against the powerfully developing attacks in networks. 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.*

Key Words: ***Artificial Intelligence, Intelligent Agents, Cyber Security, Neural Nets, Expert Systems.***

1. 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. Machine learning and Artificial Intelligence (AI) are being connected more extensively crosswise over industries and applications than any other time in recent memory as computing power, storage capacities and data collection increase. This vast measure of information can't be dealt with by people progressively. With machine learning and 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.

2. ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

In early days Computer Security and AI were not connected to each other. Artificial Intelligence researchers were interested in developing programs to decrease human work, while security professionals trying to fix the outflow of information. But the two fields have grown closer over the time, when the attacks have targeted to simulate the genuine performance, not only at the human user level but also at lower system levels. 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, could motivate the field towards more refined pattern recognition. So in the practice of trying to secure properties, such as online ticket reservations, the profitable security market is in a way stimulating advances in artificial intelligence.

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.

Artificial Intelligence practices are the key to Interference detection and make it possible to respond even to anonymous threats before spreading itself. Artificial 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.

3. ARTIFICIAL INTELLIGENCE (AI) TECHNIQUES FOR CYBER SECURITY

3.1 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. These knowledge-based systems are 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. It evaluates the current situation of the knowledge base and applies the rules relevant to that, then asserts new knowledge in to it. CSIA - Cyber Security Artificial Intelligence Expert System has the

following components in Knowledge base and Inference Engine.

Table 1: Components of Expert Systems

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

A. Security Expert System

The Security expert system follows a set of rules to battle cyber-attacks. It checks the process with the knowledge base if it is good known processes then the security system ignore otherwise the system would terminate the process. If there is no such process in knowledge base, then using inference engine algorithms (rule sets), the expert system finds out the machine state. The machine state has been composed into three states namely safe, moderate and severe. According to the machine state, the system alerts the administrator or the user about the status, and then the inference has been feed to Knowledge base.

3.2 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. It can learn any type of data. In 1957 Frank Rosenblatt created an artificial neuron (Perceptron) which paved the way for neural networks. These perceptron can learn and tackle absorbing issues by combining with other nerves i.e., perceptron. Perceptron learn on their own to identify the entity on which they are trained by learning and processing the high level raw data, as our brain learns in its own from the raw data using our sensory organ's inputs. When we apply this deep learning (trained) 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, compared with classical machine learning systems. The triumph of neural nets in cyber security is their speed. When they enforced in hardware or graphical processors it processes faster. Neural nets can permit the exact detection of new malware threats and fill in the dangerous gaps that leave organizations wide-open to attacks.

3.3 Intelligent Agents

Intelligent Agent (IA) is an independent entity which recognizes movement through sensors and follows up on an environment using actuators (i.e. it is an agent) and directs its activity towards accomplishing objectives. Intelligent agents may likewise learn or use knowledge base to accomplish their objectives. They might be extremely simple or very complex. A reflex machine, for example, thermostat is an intelligent agent. It has the behavior like understanding agent interaction language, pro-activeness and reactivity. They can adapt to real time, learn new things rapidly through communication with environment, and have memory based standard storage and recovery abilities. Intelligent agent is created in showdown against Distributed Denial of Service (DDoS) attacks. In case if there is any legal or business issue, it should be manageable to develop a "Cyber Police". Cyber Police should have mobile intelligent agents. For this we should device the infrastructure to support the quality and interaction between the intelligent agents. Multi-agent tools will give a lot of full-fledged operative appearance of the cyber police.

4. ADVANTAGES OF AI TECHNIQUES

A. Expert Systems

- Decision Support
- Intrusion Detection
- Knowledge Base
- Inference Engine

B. Neural Nets

- Intrusion Detection and Prevention System
- High speed of operation
- DoS Detection
- Forensic Investigation

C. Intelligent Agents

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

5. CONCLUSION

In this current scenario raising development in threats and cyber-attack, intelligent security system is essential.

Artificial Intelligence techniques are more flexible and robust than contemporary cyber security solutions. Therefore increasing security implementation and better defend system from a growing number of advanced and complex cyber threats. Regardless of the extreme change that Artificial Intelligence systems has conveyed to the domain of cyber security, related frameworks are not yet ready to alter completely and consequently to changes in their condition. Though we have many benefits when we use artificial intelligence techniques for cyber security, but it is not the only solution for security. When a human opponent with a clear by-passing goal attacks the intelligent security the system may fail. This doesn't means we should not use Artificial Intelligence techniques, but we should know its limits. An Artificial Intelligence technique needs continuous human communication and training. This fusion approach has many confirmed results as it works resourcefully alongside threat researchers.

6. 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.

7. REFERENCES

[1]Anderson, Frivold, Valdes, "Next- Generation Intrusion Detection Expert System (NIDES)".

[2]Rosenblatt. "The Perceptron- a perceiving and recognising automaton. Report 85-460-1, Cornell natural philosophy Laboratory, 1957.

[3]"Logic Programming for Engineering", Bratko.I, Addison-Wesley, 2001.

[6]B. Mayo, E. Tyugu, J. Penjam. Constraint Programming. Alignment ASI Series, v. 131, Springer-Verlag. 1994.

[7]E. Tyugu. Algorithms and Architectures of Artificial Intelligence.IOS Press. 2007.

[8] NabaSuroor and Syed Imtiyaz Hassan, "Identifying the factors of modern day stress using machine learning".

[9]Barika.F, K. Hadjar, and N. El-Kadhi, "ANN for mobile IDS solution," in Security and Management.

[10] TF. Lunt, R. Jagannathan. A Prototype Real-Time Intrusion-Detection Expert System.Proc.

[11] B. Iftikhar, A. S. Alghamdi, "Application of artificial neural network within the detection of dos attacks", 2009.

[12] P. Norvig, S. Russell. "Artificial Intelligence: fashionable Approach", 2000.