International Research Journal of Computer Science (IRJCS)
Issue 09, Volume 4 (September 2017)
ISSN: 2393-9842
www.irjcs.com

ARTIFICIAL INTELLIGENCE IN CYBER SECURITY – AN INVESTIGATION

[1]Harini M Rajan, [2] Dharani S
[1]Research Scholar, Savitribai Phule Pune University,Pune,India
[2]Assistant Professor, Vidhya Sagar Women's College, Kanchipuram, India

Manuscript History
Number: **IRJCS/RS/Vol.04/Issue09/SISPCS10092**
Received: 08, September 2017
Final Correction: 13, September 2017
Final Accepted: 20, September 2017
Published: September 2017
Editor: Dr.A.Arul L.S, Chief Editor, IRJCS, AM Publications, India

Abstract-- In this digital era, the explosion of internet of things and linked devices, Cyber Security experts face a lot of challenges. The experts need all the help to prevent attacks and security breaches and respond to the attacks. The number of connected 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. However, it is troublesome to develop software system with standard mounted algorithms (hard-wired logic on deciding level) for effectively defensive against the dynamically growing attacks in networks. It has become obvious that many cyber security problems is also resolved with success solely strategies of AI area unit obtaining used. This paper presents a swift survey of cyber security computing applications and analyses the views of improving the cyber security capabilities by suggesting Artificial Intelligence applications, and the already existing methods.
Keywords: Artificial Intelligence, Cyber Security, Neural nets, Expert Systems, Challenges.

I. INTRODUCTION

The increasing and progressing cyber security threat facing global businesses can be reduced by the incorporation of AI into security systems.Machine learning and artificial intelligence (AI) are being applied more broadly across industries and applications than ever before as computing power, data collection and storage capabilities increase. This vast trove of data cannot be handled by humans in real time. With machine learning and AI, that mountain of data could be whittled down in fraction of time, which helps the enterprise to identify and recover from the security threat. AI could be game changer for security teams.

II. ARTIFICIAL INTELLIGENCE

In early days Computer Security and AI were not connected to each other. AI researchers were interested in developing programs to reduce human work, while security professionals trying to fix the leakage of information. But the two fields have grown closer over the time, when the attacks have targeted to simulate the legitimate performance, not only at the human user level but also at lower system levels. CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) arevery good example of intersection of AI and Security. CAPTCHA requires the user to type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Improvements in automated 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 process of trying to secure assets, such as online ticket reservations, the commercial security market is in a way stimulating advances in AI.AI helps us in quickly identifying and analyzing new exploits and weaknesses to help mitigate further attacks and is an integral part of our solutions.

AI techniques are the key to Intrusion detection and make it possible to respond even to previously unidentified threats. AI systems that are intended to learn and adapt, and are proficient of identifying even the minutest of changes in the settings, have the potential to act much earlier – and based on vasttrove of data – than humans when it comes to grasping also novel types of cyber-attacks.

2.1 Expert Systems

An expert System is a computer system that imitates the decision making ability of a human expert. This is an example of Knowledge- based System, which is composed of two sub-systems: the Knowledge base and the Inference engine. The Knowledge base represents the instances and assertions in the real world. The inference engine is an automated reasoning system that evaluates the current scenario of the knowledge base, applies the rules relevant to that and asserts new knowledge in to it. Cyber Security Artificial Intelligence Expert System (CSIA) has the following key components in Knowledge base and Inference Engine.

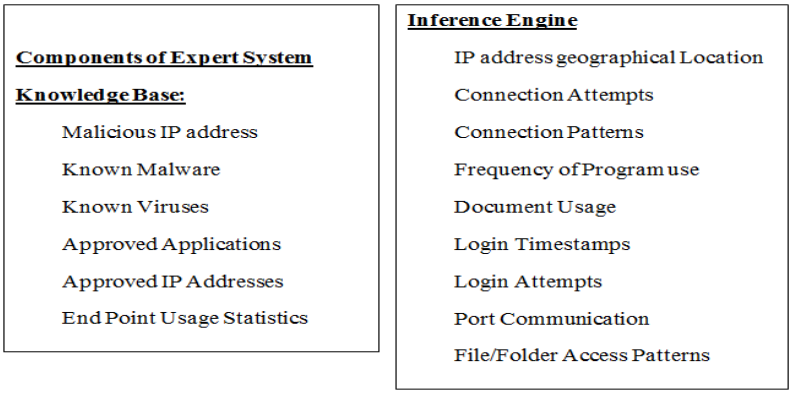

Figure 2.1 Components of Security Expert System

The Security expert system follows a set of steps to combat cyber-attacks. It checks the process with the knowledge base if it is a good known process ignore otherwise the system should terminate the process. If there is no such process in knowledge base, using inference engine algorithms (rule sets) the expert system finds the machine state. The machine state has been categorized into three; safe, moderate and severe. According to the machine state the system alerts the administrator/user and the inference has been feed to Knowledge base.

2.2 Neural Nets

Neural nets are also known as deep learning is an advanced branch of AI. It is inspired by the functions of the human brain. Our brain has several neurons, which are largely general purpose and domain-independent, can learn any type of data. In 1957 Frank Rosenblatt created an artificial neuron (Perceptron) which laid the way for neural networks. These perceptron can learn and tackle intriguing issues by combining with other perceptron. They learn on their own to recognise 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 this deep learning (trained) is applied to cyber security, the system can identify whether a file is malicious or legitimate without human intervention. This technique reveals strong results in detecting the malware, compared with classical machine learning. The success of neural nets in cyber security is their high speed when enforced in hardware or graphical processors. Neural nets can enable the precise detection of new malware threats and fill in the critical gaps that that leave organizations exposed to attacks.

2.3 Intelligent Agents

Intelligent agent (IA) is an independent entity which observes through sensors and acts upon an environment using actuators (i.e. it is an agent) and directs its activity towards achieving goals. Intelligent agents may also learn or use knowledge to achieve their goals. They may be very simple or very complex: a reflex machine such as a thermostat is an intelligent agent.They possess the behaviour: Pro-activeness, understanding agent communication language, reactivity.They can adapt to real time, learn new things quickly through interaction with environment, and have memory based exemplar storage and retrieval capabilities. Intelligent agent is developed in resistance against Distributed Denial of Service (DDoS) attacks. In case if there is any legal and business issue, it should be manageable to develop a "Cyber police" which has mobile intelligent agents. For this we should implement the infrastructure to support the quality and communication between the intelligent agents. Multi-agent tools will give a lot of complete operative appearance of the cyber police, for example a hybrid multi-agent and Agent-based distributed intrusion detection.

III. ADVANTAGES OF AI TECHNIQUES

We can use AI in various ways for cyber security. In future we may have most intelligent systems than these techniques. Even the attackers/ intruders will also use the AI for assaults.Obviously, the new developments in data understanding, illustration and handling what is more in machine learning will greatly enhance the cyber security capability of systems that may use them. The summarization of various techniques discussed in this paper is shown in the figure 2.2

AI Techniques	Advantages
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

Figure 2.2 Advantages of AI techniques

IV. CONCLUSION

In the Current scenario emerging development in malware and cyber-attacks, Intelligent Security System is needed. Contrasted with Contemporary cyber security solutions, AI techniques are more flexible and robust; therefore increasing security execution and better defend system from a growing number of advanced cyber threats. Regardless of the drastic change that AI 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 AI techniques for cyber security, AI is not the only panacea for security. When a human opponent with a clear circumvention goal attacks the intelligent security the system will fail. This doesn't means we should not use AI techniques, but we should know its limitations. AI needs continuous human interaction and training. This hybrid approach has many proven results as it works efficiently alongside threat researchers.

REFERENCES

1. E. Tyugu. Algorithms and Architectures of Artificial Intelligence.IOS Press. 2007.
2. NabaSuroor and Syed Imtiyaz Hassan, "Identifying the factors of modern day stress using machine learning", International Journal of Engineering Science and Technology, vol. 9, Issue 4, April 2017, pp. 229-234, e-ISSN: 0975–5462, p-ISSN: 2278–9510.
3. D. Anderson, T. Frivold, A. Valdes. Next-generation intrusion detection expert system (NIDES).
4. F. Rosenblatt. The Perceptron -- a perceiving and recognising automaton.Report 85-460-1, Cornell natural philosophy Laboratory, 1957.
5. I. Bratko. logic programming Programming for engineering. Addison-Wesley, 2001 (third edition). http://ieeexplore.ieee.org/document/ 4639011
6. https://business.f-secure.com/whats-the-deal-with-artificiai-intelligence-in-cyber-security
7. http://www.information-age.com/role-ai-cyber-security-123465795/
8. B. Mayo, E. Tyugu, J. Penjam. Constraint Programming. Alignment ASI Series, v. 131, Springer-Verlag. 1994.
9. F. Barika, 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," in SIN '09: Proceedings of the ordinal international conference on Security of knowledge and networks. New York, NY, USA: ACM, 2009, pp. 229–234.
12. P. Norvig, S. Russell. Artificial Intelligence: fashionable Approach. tiro Hall, 2000.
13. http://en.wikipedia.org/wiki/Expert_system.accomplished System.Wikipedia
14. https://www.sans.org/reading.../application-neural-networks-intrusion-detection-336.

