International Journal of Research in Engineering, Science and Management
Volume-1, Issue-9, September-2018
www.ijresm.com | ISSN (Online): 2581-5782

Artificial Intelligence Techniques for Cyber Security

Saket S.Kamble[1], Shahistha Khan[2], Nitin Kulkarni[3]
[1,2,3]*Student, Department of Computer Engineering, MGMCET, Navi-Mumbai, India*

***Abstract*—Today the amount of data to be processed cannot be handled securely. So, it's necessary to implement automation. It's a necessity to build software using modern methods to tackle dynamically evolving attacks in networks. This scenario can be handled using artificial intelligence to provide faster recovery and flexibility over manual handling of precious data. Artificial Intelligence technique can improve overall security and give better authentication and authorization to external threats. Beside this AI provides great opportunity for cyber security, its utilization has legitimate risk and concern. To promote the increment in development of cyber security, AI has a significant contribution with human knowledge, and its way to respond the human behavior. Thus we can use AI capabilities for reducing the risk of threats to the valuable data.**

***Index Terms*—Artificial Intelligence, Cyber Security**

I. Introduction

Cyber-attacks at time could be irrevocable vandalism to business, thus making security as most important and valuable asset for companies and individuals, yet most vulnerable to threats. So it's absolutely crucial that for getting authorized access without and data breach to the database.

Artificial intelligence can play a major role in cyber security .Large data with probability of risk can't be dealt with conventional ways. With AI at the apex of current technology can and process human behavior making it prone to the importance of data the system has and how the system can be hacked, thus making it difficult for the intruder to look into the system.

II. Need for Cyber Security

Cyber Security has always been the matter for concern even with the most secured system and techniques. And because of attacker evolving every day with new cyber attacking techniques, it is certain to define cyber security that constitute a mechanism to defend the attack.

Commercially the world wide investment on cyber security has grown from 71.1 billion in 2014 and (7.9% over 2013), and 75 billion in 2015 (4.7% from 2014) and expected to reach 101 billion by 2018.Companies are starting to understand that it has become very easy for the any one to be attacker since malware is a publicly available commodity, and thus the companies in cyber security domain has improved drastically providing solution for defending against attack.

III. Artificial Intelligence in Cyber Security

In the earlier days Cyber security was not really connected with the Artificial intelligence. Moreover researches were more interested in developing programs that will reduce the human work, while security professionals were trying to fix the intrusion of information. However over the time attackers has also evolved ,targeting the genuine system performance ,not only at human using level but at lower machine level as well. One of the most common example is CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is. It involves generating a machine generated key, which is supposed to be inserted as a security check for login, along with prerequisite knowledge.AI thus can detect the anonymous threats before spreading itself. Artificial intelligence system are prone to learn ,improve itself and adapt changes ,with potential to act much earlier and analyze different types of cyber –attack.

IV. AI Technique for Cyber Security

A. Expert System

Expert system is the most widely used tool .It is a software which helps to reply for the inquiries made by client or by other software. It can be used for decision support, the best example is medical diagnosis. Expert System includes a Knowledge base and inference engine .Knowledge system represent the illustrations and affirmation in the real world. Interface system is an automatic reasoning system. It evaluates the existing knowledge in the system and assert the new knowledge feed it to the existing one. Empty Knowledge base and inference engine are together called expert system shell. Expert system along with improving knowledge also supports extra functionality for simulation, for making calculation etc. The most importance of Expert system is its feature to knowledge acquisition problem that is crucial in developing real applications.

B. Neural Nets

Neural Nets is also known as deep learning. Neural network is an information processing technique which is inspired by biological working of human nervous system. The most significant thing about this technique is the novel structure of processing information. This process is composed of large

number of highly interconnected processing element called neurons, working in union to solve specific problem.

When we apply this neural nets technique to cyber security, the system will be easily able to identify whether the file is legitimate or not without human interference. This technique yields a strong result in detecting the malicious threats, compared with classical machine learning technique. The neural nets is so effective because of the faster processing than any other system. Neural network can perform exact detection of new malicious content and threats and bridge the gap for organizations for its exposure to attacks.

C. Intelligent Agents

Intelligence Agent are software application that retrieves, searches and performs action accordingly .It is an entity which takes data using sensor and acts upon an environment using actuators to achieve goal. The agents may lean for the goal which may be complex or simple. This application are automated and uses internet to retrieve data automatically. When the relevant information is found, the agent extract and list that data. The collected data is given as report to the user.

Intelligent agents can adapt to real time, learn new things rapidly from its environment .Intelligence agent are to prevent Distributed Denial of Services (DDoS) attacks. Also it can be used for solving legal case or business issues, if required can be helpful for Police, and even can be helpful in developing a "Cyber Police". For Cyber Police a proper infrastructure, database and system need to be maintained to provide quality interaction between intelligence agents.

V. Application of Cyber Security

- Faster processing
- Unauthorized intrusion detection and Prevention
- DDOS Detection
- Mobility
- Proactive
- Proactive and Reactive
- Botnet Detection
- Spam Filter Application
- Secured User authentication

VI. Conclusion

In today's situation of rapid growing intelligence of malware and unwanted attacks, it is necessary to develop a strong defence mechanism. Thus Analysis of article shows that Artificial intelligence is most required security method to be applicable for a Good secured system with good commercial profits.

References

[1] https://www.normshield.com/cyber-security-with-artificial-intelligence-in-10-question/
[2] https://en.wikipedia.org/wiki/Intelligent_agent/
[3] V. Chatzigiannakis, G. Androulidakis, B. Maglaris. A DIS Prototype Using Security Agents
[4] J. Bai, Y. Wu, G. Wang, S. X. Yang, and W. Qiu, "A novel intrusion detection model based on multi-layer self-organizing maps and principal component analysis
[5] L. DeLooze, Attack Characterization and Intrusion Detection using an Ensemble of SOM
[6] D. Stopel, Z. Boger, R. Moskovitch, Y. Shahar, and Y. Elovici, "Application of artificial neural networks techniques to computer worm detection".