International Journal of Progressive Research in Science and Engineering
Volume-1, Issue-3, June-2020
www.ijprse.com

Technology to Combat Cyber Attacks by Artificial Intelligence

Anirban Chakraborty

Student, Department of Artificial Intelligence, Lovely Professional University, Phagwara, Punjab, India.

Corresponding Author: anirbanchakraborty456@gmail.com

Abstract: - Cyber protection is obviously the discipline that will profit almost everyone from the introduction of AI. This is challenging to render a proposal to defend from strong system assaults. The usage of artificial intelligence techniques will help a lot. Where the weakness and slowness of conventional defence systems might be, artificial intelligence approaches may boost their complete implementation of the security program and provide dramatically improved protection against a growing range of cyber threats. While AI's information protection policies provide positive incentives, their usage has legitimized fears and threats. In order to promote better cyber protection initiatives, an alternate viewpoint of cyber earth connections is required where AI is reinforced with human consciousness, because neither people nor AI alone have historically proven to be effective in this specific field. Socially cautious use of AI approaches to mitigate more associated problems and risks is therefore necessary.

Key Words: — ***Cyber security, Artificial Intelligence (AI), Security intelligence, Cyber defence, Denial of Service (DoS), Self-Organizing Maps (SOM).***

I. INTRODUCTION

The security mechanism needs to cooperate continuously with alteration players, risks and the atmosphere in the online game to ensure consistent and scalable health. Cyber fact, as it may be, is distinguishable in any quantity. Safety methodologies are frequently implemented in order to modify documented attacks, and even since the protection system is unsolid and fluid, it cannot usually respond to shift within its scope example, modification methods can be ineffective and sluggish even for individual experiences.

Artificial intelligence approaches may help to overcome a range of limitations of modern information protection techniques, due to their adaptable and versatile device behavior. While the information protection of AI is dramatically enhanced, you may notice the same worry. Many people find AI to be a rising human existential threat. Likewise, lawyers and scientists are cautious regarding the position of auto-governing. AI is able to concentrate on how the mind works, and even how humans know, evaluate, and then act as they attempt to tackle a issue. Before this they use the final outcome of this test to build smart systems and software [1].

The motivation behind this initiative is to highlight the absence of conventional protection controls and also the success that has been achieved to date on information security using AI approaches. Moreover, this role decreases the risks and issues associated with this particular growth, analyzing the current circumstances of AI, retaining problems and outlines the future

Fig.1. Artificial Intelligence

IJPRSE
Progressive Research
International Journal of Progressive Research in Science and Engineering
Volume-1, Issue-3, June-2020
www.ijprse.com

II. APPLICATIONS OF AI TECHNIQUES

I also defined utilizing numerous AI approaches in order to prevent cyber-attacks in this specific region. As we learn, we are preparing toward a near future, where we communicate with a computer that is smarter than us. As the approaches still build risks and attack every day, we need to implement AI tactics inside our defense framework to determine this specific attack.

A. Application of Intelligent Agents

Smart agents are self-sustaining computer network powers that speak to one another to relay information and often include one another in organizing and updating the appropriate responses to unpredictable incidents. Their strength, their endurance and, under the conditions, their synergistic nature are a technology of intelligent agents that can combat cyber-attacks.

Intelligent agents (distributed denial of service) are used to respond to assaults by DDoS. A specific standard of cyber protection, which includes intelligent (portable) components, will be possible after solving various legal and business problems. Deployment of infrastructures is important to support the cyber worker's communications and transport; however, enemies cannot access them. For example, the neural network intrusion detection and the combined Multi-Agent Strategies, a multi-agent protocol is currently suggested for the full organizational representation of the cyberspace. In [3], a detection of intrusion is detected, primarily on a central worker.

B. Application of Neural Networks

The creation of Frank Rosenblatt's perceptron in 1957 marked the beginning of a past neural network-an artificial neuron is known as essential neural net ingredients [4]. Perceptions can explore and work with complex problems by introducing small numbers. In the neural network there are massive man-made neurons. Neural networks have the advantage of significantly simultaneous thinking and decision taking. The working level is generally known to them. Their algorithm is ideal for the identification of trends, schemes, attack reactions [5] etc. We still help the software or even the deployment of equipment. The identification and elimination of intrusion is achieved utilizing neural networks [6 10]. They are suggested for use in the recognition of marks, the analysis of zombies and spam, as well as the diagnosis of viruses and laptop-worms, and in forensic testing [11,13].

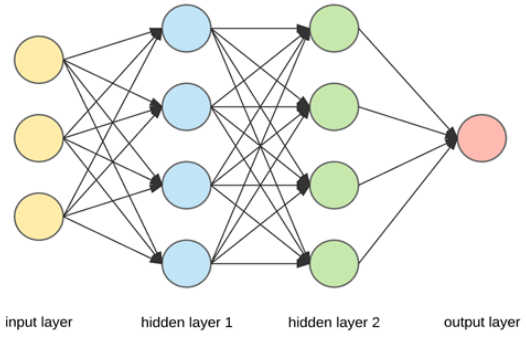

Fig.2. Neural Networks

The fast speed of the neural network, when built on equipment, or even as a graphics processing feature, is popular in cyber defence. Different recent advances in the ground breaking 3G neural networks of the neural network – in this specific biological neurons, various domain opportunities are more prudently imitated by neural nets. The use of Field Programmable Gate Arrays (FPGA) allows it possible to develop neural networks and to adjust them to growing threats rapidly.

C. Application of Expert Methods

Expert phone program is the most widely used AI tool. It is a software system that tries to find answers to consumer or maybe an external application queries of use of finance, scientific research and cyberspace, direct application of the service of preference. There are expert structures of various forms, from simple programs for research to integrated models, which are efficient and extremely broad for solving complicated problems.

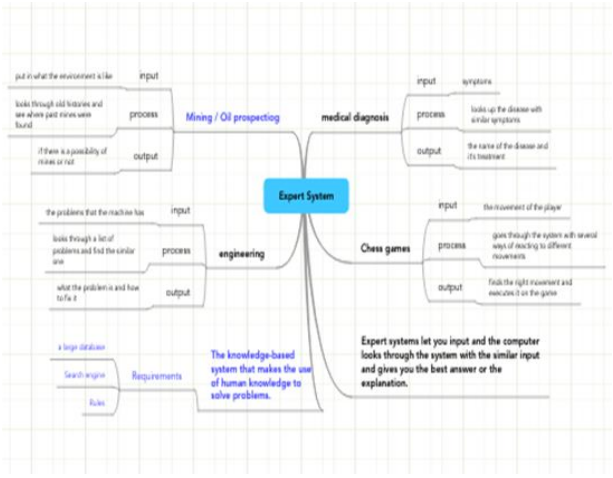

Fig.3. Expert System

A professional information base for a specific application field comprises of a pro method. In fact, it provides an inference mechanism for weaker knowledge and for further details concerning a situation depending on the current understanding. The shell of the expert framework contains the empty information base and even the deduction motor that must be assembled before it can be used. The professional process shell is to be provided, in addition to experience in client collaboration programs and in different technologies that are required by hybrid pro frameworks, in the information base software package Professional process shell.

The expert method is built for cyber security safety. It will help to commit protection measures and direct the optimal usage of restricted quantities of resources. The usage of intrusion prevention specialist approaches is established [14, 15].

Knowledge base, other settings and rule sets where expert system resides are important for detecting intrusion details in the Network. Different network attack features are contained in a database containing the relevant base of knowledge, and displayed as a part of the site system. It is important to transfer the theory set successfully in real-time data packets. The rules may also be obtained from the servers and managed utilizing the program infrastructure

D. Application of Deep Learning

Through machine learning includes computer techniques for completely new understanding, fresh new expertise, and even improved approaches for improving current information. The gap in the masters degree would rely on their sophistication, from simple parametric learning to complicated ways of abstract thinking, to analogy, concept thinking and also functional learning, grams and operations. Monitored and unattended instruction can also be utilized.

Fig.4. Deep Learning

For massive amounts of knowledge, unsupervised learning is quite necessary. This is precisely where vast logs can be obtained in the cyber security sector. The idea of data mining was unmonitored learning in AI. Unattended research, in some situations, from Self-Organizing Maps (SOM) can also be a benefit of neural nets[10, 16, 13, 17].

A kind of learning strategies are concurrent algorithms and are distributed to scalable hardware. Such learning methods are described by neural networks and genetic algorithms. For examples, fuzzy logic and genetic algorithms are still used in the methods of risk detection as seen in [18]. Few systems such as [19, 20, 21] have been introduced.

III. FUTURE ISSUES CONSIDERATION

The major gap between accelerated targets and long-term expectations must be understood, if you foresee the potential research and implementation and growth of cyber-attack protection of AI strategies. Many AI techniques are sufficient to determine cyber-assault, although other actual cyber-assault challenges are usually important to take advanced action.

One may see the usage of completely different skill criteria in decision-making. Such requirements provide a structured and functional system of knowledge in the decision taking of a project. The automated information management system offers rapid assessments of situations that provide leaders and policy makers with a dominance over some C2 degree defence.

As already employed in a few projects, specialist approaches frequently conceal the existence of their technology inside the same environment as the framework for safety-planning function.

Expert strategies would provide more complex systems because large bases of expertise are built in the future. In order to obtain this unique jobs expertise, significant acquisitions would be required, as well as broad scalable information bases. The implementation of the professional approach would entail more improvement: equipment with modularity should be included and hierarchical information bases will also be included in the specialist process.

IV. APPLICATION OF AI TECHNIQUES AND THEIR ADVANTAGES

The application of AI techniques and their advantages are summarized in Table 1.

Table.1. AI techniques and their usage

AI Techniques	Usage
Intelligent Operator	Proactive Agent communication language
	Reactive
	Defence against DDoS
	Mobility
Application of Neural Nets	For intrusion detection and prevention system,
	Very high speed of operation,
	For DoS detection,
	For Forensics Investigation
	Warm detection
Application of Expert System	For decision support For Network Intrusion Detection
	Knowledge base
	Inference engine
Application of Learning	Machine learning
	Supervised and unsupervised learning.
	Malware detection, intrusion detection.
	Self-Organizing Maps (SOM)

V. CONCLUSION

In addition to computer protection, AI is recognized as one of the most important advances in the digital era. The global safety showcase must also be followed by other approaches, an algorithm, services, and organizations that provide solutions focused on AI. Such application structures aim to be more adaptable, stable and versatile, enhancing protection implementation as well as better defending the network against the increasing range of sophisticated cyber threats in comparison to traditional data safety approaches. Today, the most persuasive and efficient instruments in AI's domain name are deep learning methods. Among other areas in which the latest innovation is not just the neural networks, the usage of clever cyber security technologies is often significant. Nobody or AI alone has shown a standard information security success since recently. Regardless of the enormous improvements AI has rendered to cyber-security domain name, the systems are not prepared to alter their situation adequately and absolutely. A comprehensive view of the cyber world of partnerships is also important.

REFERENCES

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

[2]. E. Herrero, M. Corchado, A. Pellicer, A. Abraham, "Hybrid multi agent-neural NIDS with MV".

[3]. V. Chatzigiannakis, G. Androulidakis, B. Maglaris. A DIS Prototype Using Security Agents.

[4]. F. Rosenblatt. The Perceptron a perceiving and recognizing automaton.

[5]. G. Klein, A. Ojamaa, P. Grigorenko, M. Jahnke, E. Tyugu. Enhancing Response Selection in Impact Estimation Approaches

[6]. 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.

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

[8]. D. A. Bitter, T. Elizondo, Watson. Application of ANN and Related Techniques to Intrusion Detection.

[9]. R.-I. Chang, L.-B. Lai, W. D. Su, J. C. Wang, and J.-S. Kouh, "Intrusion detection by backpropagation neural networks with sample-query and attributequery,"

[10]. L. DeLooze, Attack Characterization and Intrusion Detection using an Ensemble of SOM.

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

[12]. D. Stopel, Z. Boger, R. Moskovitch, Y. Shahar, and Y. Elovici, "Application of artificial neural networks techniques to computer worm detection".

[13]. B. Fei, J. Eloff, MS Olivier, H. Venter. The use of self-organizing maps of anomalous behavior detection in a digital investigation. Forensic Science International, v. 162, 2006, pp. 33-37.

[14]. D. Anderson, T. Frivold, A. Valdes. Next-generation intrusion detection expert system (NIDES).

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

[16]. 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.

[17]. V. K. Pachghare, P. Kulkarni, D. M. Nikam. Intrusion Detection System using Self Organizing Maps.

[18]. R. Hosseini, J. Dehmeshki, S. Barman, M. Mazinani, S. Qanadli. A Genetic Type-2 Fuzzy Logic System for

Pattern Recognition in Computer Aided Detection Systems.

[19]. Naba Suroor 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.

[20]. Syed Imtiyaz Hassan, "Designing a flexible system for automatic detection of categorical student sentiment polarity using machine learning", International Journal of u- and e- Service, Science and Technology, vol. 10, no.3, Mar 2017, pp. 25-32, doi: 10.14257/ijunesst.2017.10.3.03, ISSN: 2005-4246.

[21]. Syed Imtiyaz Hassan, "Extracting the sentiment score of customer review from unstructured big data using Map Reduce algorithm", International Journal of Database Theory and Application, vol. 9, issue 12, Dec 2016, pp. 289-298, doi:10.14257/ijdta.2016.9.12.26, ISSN: 2005-4270.