International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 5 (2017), pp. 883-889

http://www.ripublication.com

Applying Artificial Intelligence Techniques to Prevent Cyber Assaults

Amaan Anwar[1] & Syed Imtiyaz Hassan[2]

[1,2]*Department of Computer Science and Engineering*

Jamia Hamdard (Hamdard University), New Delhi-62, India

Abstract

Cyber security ostensibly is the discipline that could profit most from the introduction of Artificial Intelligence (AI). It is tough to make software for defending against the powerfully developing assaults in systems. It can be cured by applying techniques of artificial intelligence. Where conventional security systems may be slow and deficient, artificial intelligence techniques can enhance their overall security execution and give better security from an expanding number of complex cyber threats. Beside the great opportunities attributed to AI inside cyber security, its utilization has legitimized risks and concerns. To promote increment the development of cyber security, a holistic perspective of associations cyber environment is required in which AI is consolidated with human knowledge, since neither individuals nor AI alone has proven overall success in this sphere. In this manner, socially mindful utilization of AI techniques will be needed to further mitigate related risks and concerns.

Keywords: Cyber security, Artificial Intelligence (AI), Security intelligence, Cyber defense, Denial of Service (DoS), Self-Organizing Maps (SOM).

1. INTRODUCTION

To execute versatile and persistent protection, security system need to continually conform to changing environment, threats and actors involved in the digital play. Cyber reality, be that as it may, shows up to some degree distinctive. Security methodologies are routinely custom fitted to known assaults, and because of the absence of flexibility and robustness, security framework ordinarily can't adjust consequently to change in

their encompassing. Indeed, even with human interaction, adaption processes are likely to be slow and insufficient.

Due to their flexible and adaptable system behavior artificial intelligence techniques can help defeat different deficiencies of today's cyber security tools. Although AI has already significantly enhanced cyber security, there are likewise genuine concern. Some see AI as a developing existential hazard for mankind. Likewise, scientist and legal expert have expressed caution at the expanding role that self-governing AI substances are playing in the cyberspace and have raised worries about their moral reasonability. AI is proficient by concentrate how human brain thinks, and how people learn, choose, and work while attempting to tackle an issue, and after that utilizing the results of this review as a premise of creating intelligent software and systems [1].

The motivation behind this work is to highlight the deficiencies of conventional security measures and additionally the advance that has been made so far by applying AI techniques to cyber security. Furthermore this works compresses the dangers and concern connected to this advancement, by investigating AI's existing conditions, tending to present concerns, sketching out heading for what's to come.

2. APPLICATIONS OF AI TECHNIQUES

In this section I have discussed the utilization of various AI techniques to prevent cyber assault. As we know that we are moving towards a future in which we will interact with machine which will be smarter than human beings. As the technologies are developing day by day likewise the threats and assault are also enhancing to fight against this assault we need to implement AI techniques in our security system.

2.1. Application of Intelligent Agents

Intelligent agents are self-sufficient computer system created force that communicate with each other to share information and participate to each other so as to arrange and actualize proper reactions if there should arise an occurrence of unforeseen occasions. Their mobility and adaptability in the conditions they are conveyed in, and in addition their synergistic nature, intelligent agent technology appropriate for fighting cyber assaults.

Intelligent agents is utilized in resistance against Distributed Denial of Service (DDoS) assaults. In the wake of settling some lawful and furthermore business issues, it ought to be conceivable on a basic level to build up a cyber-police which comprises of intelligent agents (portable). Installation of infrastructure is required to support the cyber agent’s movement and communication, however should be inaccessible for foes. For entire operational picture of the cyber space a Multi- agent tools is required, for example, a neural network-based intrusion detection and hybrid multi-agent techniques already proposed in [2]. An agent based distributed intrusion detection is depicted in [3].

2.2. Application of Neural nets

After the creation of perceptron by Frank Rosenblatt in 1957 Neural nets history starts – an artificial neuron is considered as important components of neural nets [4]. Perceptions can learn and tackle intriguing issues by joining in limited numbers. While countless artificial neurons are present in neural nets. Thus usefulness of greatly parallel learning and decision-making is provided by neural nets. They are known by the operation speed. Their application is for learning pattern recognition, for arrangement, for choice of reactions to assaults [5] and so forth. They support either in software or in hardware installation. Neural nets are used to carry out the detection and prevention of intrusion [6-10]. Recommendations are there to utilize them in DoS identification, malware classification, spam recognition, zombie detection, and computer worm identification and in forensic investigations [11-13].

Neural nets are famous in cyber defense because of its high speed, when installed in hardware or as a graphic processors component. Various new advancements noticed in the neural nets innovation- 3G neural nets – in this biological neurons are more sensibly mimicked by neural nets, various application openings granted. By the utilization of Field Programmable Gate Arrays (FPGA) great advancement is reported such that it empower fast improvement of neural nets and their conformity to changing threats.

2.3. Application of Expert systems

As we know the most commonly used AI tool is Expert system. It is a software which helps in discovering answers to inquiries presented either by a client or by another software. Direct utilization in decision support for example, in finances, in medical diagnosis, or in cyberspace. Expert systems are present in different forms from small system for diagnostic purpose to hybrid system which is for solving complex problems this system is exceptionally large and powerful.

An expert system comprises knowledge base in which expert knowledge is stored regarding a particular application domain. It also incorporates an inference engine for inferring answers in light of present knowledge and also further knowledge about a circumstance. Expert system shell consist of empty knowledge base and inference engine, before its utilization knowledge must be loaded. For including knowledge in the knowledge base software must support Expert system shell, and it can be stretched out with programs for client cooperation's, and with different programs that might be utilized as a part of hybrid expert systems.

Expert system is for security arranging in cyber defense. It helps in determination of safety efforts, and gives direction for ideal use of resources which are limited in quantity. Expert systems utilization in intrusion detection is already known [14, 15].

To detect Network Intrusion information which are required are Knowledge Base, Rule sets and other configurations on which Expert System run. Different network intrusion behavior specific feature are stored in knowledge base, and are collected from database which contains related knowledge base and are stored as the web application part. It is

necessary for Real-time data packets to pass the rule set. These rule sets are also collected from Database and are preserved for the application infrastructure.

2.4. Application of Learning

In machine learning, it involves computational strategies for procuring new knowledge, and also new aptitudes and better approaches to compose existing knowledge. The variation of learning problem depends upon their complexity from simple parametric learning to complicated forms of symbolic learning, for illustration, learning of concepts, even learning of behavior, grammars, and functions. Supervised as well as unsupervised learning can be used.

Unsupervised learning is particularly valuable for large amount of data. This can be seen in cyber defense where expansive logs can be gathered. Unsupervised learning in AI gave the concept of data mining. Also a usefulness of neural nets can be Unsupervised learning, in specific, of Self-Organizing Maps (SOM) [10, 13, 16, 17].

Parallel learning algorithms that execution on parallel hardware is a type of learning methods. Genetic algorithms and neural nets are used to represent these learning strategies. Genetic algorithms and fuzzy logic has been, for example, utilized as a part of threat detection systems portrayed in [18]. Few such application has been implemented by [19, 20, 21].

3. FUTURE ISSUES CONSIDERATION

One must be aware of the difference between immediate goals and long term viewpoints, when predicting the future work and expansion and application of AI techniques in cyber assault prevention. Many AI techniques are relevant in cyber assault prevention, also there are many current cyber assault problems that need more sophisticated measures.

One can observe utilization of totally new standards of knowledge dealing with decision making. These standards in the decision making software incorporate a modular and hierarchical knowledge architecture. To ensure fast circumstance evaluation that provide leaders a decision superiority and decision makers on any C2 level security [22] is only provided by automated knowledge management.

Expert systems are as of now being utilized as a part of numerous applications, its presence inside an application is sometimes hidden, same as the software like safety efforts planning software.

If in future large knowledge bases will be created, expert systems will get more extensive application. For this purpose knowledge acquisition will require extensive investment, and large modular knowledge bases must be developed. The expert system innovation will require advancement further: in the expert system tools presence of modularity is must and also make use of hierarchical knowledge bases.

4. 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
Application of Intelligent Agent	• Proactive • Agent communication language • Reactive • Defense 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)

5. CONCLUSION

AI is considered as a standout amongst the most encouraging advancement in the information age and cyber security. New techniques, algorithm, tools and enterprises offering AI based services are always rising with respect to the worldwide security showcase. Contrasted with traditional cyber security solutions, these frameworks are more adaptable, flexible and robust, therefore enhancing security execution and better protect system from an expanding number of refined cyber threats. Right now, profound learning procedures are potentially the most encouraging and effective tools in the domain of AI. There is additionally an earnest requirement for use of intelligent cyber defense methods in a various areas where the most appropriate technology is not only neural nets. As of recently, neither individuals nor AI alone have demonstrated general achievement in cyber security. Regardless of the immense 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. In addition a holistic view on the cyber environment of associations is required.

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 attribute-query,"

[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.

[22] C2-level Security, [Online: Available], https://msdn.microsoft.com/en-us/library/windows/desktop/aa376387(v=vs.85).aspx