Tushar Aggarwal, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 10, Issue 12, (Series-I) December 2020, pp. 41-44

RESEARCH ARTICLE OPEN ACCESS

Artificial Intelligence Techniques to Prevent Cyber Crime

Tushar Aggarwal[1], Er. Pooja Kapila[2]
[1]*Department of Computer Science & Engineering*
(Chandigarh Group Of Colleges Jhanjeri , Mohali),Chandigarh , India
[2]*Assistant Professor (Department of Computer Science)*
(Chandigarh Group Of Colleges Jhanjeri , Mohali),Chandigarh , India

ABSTRACT
The world is going digital at an unprecedentedly fast pace, and the change is only going to go even faster. The digitalization means everything is moving at lightning speed – business, entertainment, trends, new products, etc. The consumer gets what he or she wants instantly because the service provider has the means to deliver it. A typical cyber-attack is an attempt by adversaries or cybercriminals trying to access, alter, or damage a target's computer system or network in an unauthorized way. It is systematic, intended, and calculated exploitation of technology to affect computer networks and systems to disrupt organizations and operations reliant on them. While the future seems bleak, there have also been developments in technology with significant impacts on cybersecurity. One such major game-changer in the field of cybersecurity is tools and techniques developed and supported by Artificial Intelligence (AI) and Machine Learning (ML) as a subset of it.

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

Date of Submission: 24-11-2020 Date of Acceptance: 07-12-2020

I. INTRODUCTION

Artificial Intelligence is no longer just a buzzword and is being used extensively in industries of all kinds. Customer service, education, automation, etc. are only some of the many sectors where AI has instigated advancement by leaps and bounds. It is also playing a significant role in the ongoing fight against cybercrime.
Following are some of the ways Artificial Intelligence (AI) and Machine Learning (ML) are making a difference by giving the much-needed boost to cybersecurity.

1. Machine Learning In Cyber Threat Detection

Organizations have to be able to detect a cyber-attack in advance to be able to thwart whatever the adversaries are attempting to achieve. Machine learning is that part of Artificial Intelligence which has proven to be extremely useful when it comes to detecting cyber threats based on analyzing data and identifying a threat before it exploits a vulnerability in your information systems. 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.

➢ APPLICATIONS OF AITECHNIQUES

InthissectionIhavediscussedtheutilizationofvariousAItechniquestopreventcyber assault.Asweknowthatwearemovingtowardsafuturei nwhichwewillinteractwith machine which will be smarter than human beings. As the technologies aredeveloping day by day likewise the threats and assault are also enhancing to fight against this assault we need to implement AI techniques in our securitysystem.

➢ Application of IntelligentAgents

Intelligent agents are a new paradigm for developing software applications. More than this, agent-based computing has been hailed as 'the next significant breakthrough in software development' (Sargent, 1992), and 'the new revolution in software' (Ovum, 1994). Currently, agents are the focus of intense interest on the part of many sub-fields of computer science and artificial intelligence. Agents are being used in an increasingly wide variety of applications, ranging from comparatively small systems such as email filters to large, open, complex, mission critical systems such as air traffic control. At first sight, it may appear that such extremely different types of system can have little in common. And yet this is not the case: in both, the key abstraction used is that of an agent. Our aim in

this article is to help the reader to understand why agent technology is seen as a fundamentally important new tool for building such a wide array of systems. More precisely, our aims are five-fold:
• to introduce the reader to the concept of an agent and agent-based systems.
• to help the reader to recognize the domain characteristics that indicate the appropriateness of an agent-based solution.
• to introduce the main application areas in which agent technology has been successfully deployed to date.
• to identify the main obstacles that lie in the way of the agent system developer, and finally.
• to provide a guide to the remainder of this book.

➢ Application Of Neural Nets

An artificial neuron is considered as important components of neural nets . Perceptionscanlearnandtackleintriguingissuesbyjoining inlimitednumbers.While countlessartificialneuronsarepresentinneuralnets.Thusefulnessofgreatlyparallel 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, forchoiceofreactionstoassaultsandsoforth.Theysupporteitherinsoftwareorin hardware installation. Neural nets are used to carry out the detection and prevention of intrusion . Recommendations are there to utilize them in DoS identification, malware classification, spam recognition, zombie detection, and computer worm identification and in forensic investigations.

➢ Neural Network for Deep Learning

1) Following Neural Network, architectures are used in Deep Learning
2) Feed-forward neural networks
3) Recurrent neural network
4) Multi-layer perceptrons (MLP)
5) Convolutional neural networks
6) Recursive neural networks
7) Deep belief networks
8) Convolutional deep belief networks
9) Self-Organizing Maps
10) Deep Boltzmann machines
11) Stacked de-noising auto-encoders

➢ 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 systemfordiagnosticpurposetohybridsystemwhichisforsolvingcomplexproblems this system is exceptionally large andpowerful.

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.

➢ Application ofLearning

Today, machine learning is different from what it used to be in the past, due to the emergence of advanced computing technologies. Initially, it had gained momentum due to pattern recognition and the fact that computers did not have to be programed to execute certain tasks to learn. Many researchers who were interested in Artificial Intelligence (AI) investigated this area further to find out whether computers could really learn from data or not.

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) .

➢ FUTURE ISSUESCONSIDERATION

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 techniquesincyberassaultprevention.ManyAItechniquesarerelevantincyberassault prevention, also there are many current cyber assault problems that need more sophisticatedmeasures.
Onecanobserveutilizationoftotallynewstandardsofknowledgedealingwithdecision making. These standards in the decision making software incorporate a modular and hierarchical knowledge architecture. To ensure fast circumstance evaluation that provideleadersadecisionsuperiorityanddecisionmakersonanyC2levelsecurity 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,andlargemodularknowledgebasesmustbe developed.Theexpertsystem innovation will require advancement further: in the expert system tools presence of modularity is must and also make use of hierarchical knowledgebases.

➢ APPLICATION OF AI TECHNIQUES AND THEIRADVANTAGES

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 ➢ Mobility ➢ Rationality ➢ Adaptability ➢ Collaboration
Application of Neural Nets	● For intrusion detection and preventionsystem, ● Very high speed ofoperation, ● For DoSdetection, ● For ForensicsInvestigation ● Warmdetection
Application of Expert System	● For decisionsupport ● For Network Intrusion Detection ● Knowledgebase ● Inference engine
Application of Learning	● Machinelearning ● Supervised and unsupervisedlearning ● Malware detection, intrusiondetection ● Self-Organizing Maps(SOM)

II. 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 protectsystemfromanexpandingnumberofrefinedcyberthreats.Rightnow,profound learning procedures are potentially the most encouraging and effective tools in the domain of AI. The fast development of information technology had a lot of positive impact and brought many conveniences into our lives. However, it also caused issues that are difficult to manage such as the emergence of cyber crimes. As the technology continues to evolve, criminal cases change correspondingly. Every day we are faced with increasing number and variety of cyber crimes, since this technology presents an easy way for criminals to achieve their goals. Critical infrastructures are especially vulnerable. Application of AI techniques are already being used to assist humans in fighting cyber crimes, as they provide flexibility and learning capabilities to IDPS software. It has become obvious wide knowledge usage in decision making process requires intelligent decision support in cyber defense which can be successfully achieved using

AI methods. Available academic resources show that AI techniques already have numerous applications in combating cyber crimes. This paper has briefly presented advances made so far in the field of applying AI techniques for combating cyber crimes, their current limitations and desired characteristics, as well as given the scope for future work

REFERENCES

[1]. Artificial Intelligence Techniquesto Prevent Cyber Assaults Guide by Miss Er. Pooja Kapila(Ass.Professor) Department Of Computer Science (CGC Technical Campus)

[2]. D.Stopel,Z.Boger,R.Moskovitch,Y.Shahar,a ndY.Elovici,"Applicationof artificial neural networks techniques to computer wormdetection".

[3]. B. Stahl, D. Elizondo, M. C. Mayer, Y. Zheng, K. Wakunuma, (2010) "Ethical and Legal Issues of the Use of Computational Intelligence Techniques in Computer Security and Computer Forensics", International Joint Conference on Neural Networks (IJCNN).

[4]. N. C. Rowe, "Counterplanning Deceptions To Foil Cyber-Attack Plans", Proceedings of the 2003 IEEE Workshop on Information Assurance, United States Military Academy, West Point, Information Assurance Workshop.

[5]. Ionita, L. Ionita, (2013) "An agent-based approach for building an intrusion detection system," 12th International Conference on Networking in Education and Research (RoEduNet).

[6]. B. S. Fisher, S. P. Lab, (2010) Encyclopedia of Victimology and Crime Prevention, SAGE Publications, Vol. 1, pp. 251, USA

[7]. J. S. Russell, P. Norvig, (2003) Artificial Intelligence: A Modern Approach, 2nd edition, Upper Saddle River, Prentice Hall, New Jersey, USA.

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