**Applying Artificial Intelligence Techniques to Prevent Cyber Assaults**

**INTRODUCTION**

Cyber security ostensibly is the discipline that could profit most from the introduction of Artificial Intelligence (AI).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 is valuable fodder for AI, which can process and analyze everything captured to understand new trends and details. For cyber security, this means new exploits and weaknesses can quickly be identified and analyzed to help mitigate further attacks. It has the ability to take some of the pressure off human security “colleagues.” They are alerted when an action is needed, but also can spend their time working on more creative, fruitful endeavors [1] .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 changein 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 [2].

**PROBLEMS**

1. Conventional security systems are slow and deficient.

2. It is tough to make software for defending against the powerfully developing assaults in systems.

3. Every day hackers release new malware into “the wild”, as many as 50,000 new threats each day. There is simply no way an security system can update its threat list fast enough.

**OBJECTIVES**

1. 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.

2. To compress the dangers and concern connected to this advancement, by investigating AI's existing conditions, tending to present concerns.

3. To integrate AI’s some most important application for preventing cyber assault.

**METHODOLOGIES**

In this section we will discuss 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.

**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 [3]. An agent based distributed intrusion detection is depicted in [4].

**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 [5]. 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 [6] and so forth. They support either in software or in hardware installation.

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.

**Application of Expert System**

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.

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 [7, 8]. 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.

**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) [9, 10, 11, 12]. 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.

**PROPOSED SOLUTION**

1. Learn user behavior through the entire session by machine learning.

a) How it logged in,

b) Interaction between different type of user and so on.

2. If find any violation of expected behaviors it will communicate with intelligent agent.

a) Intelligent agents share the information on the server,

b) Communicate with other intelligent agents to participate in a checking procedure,

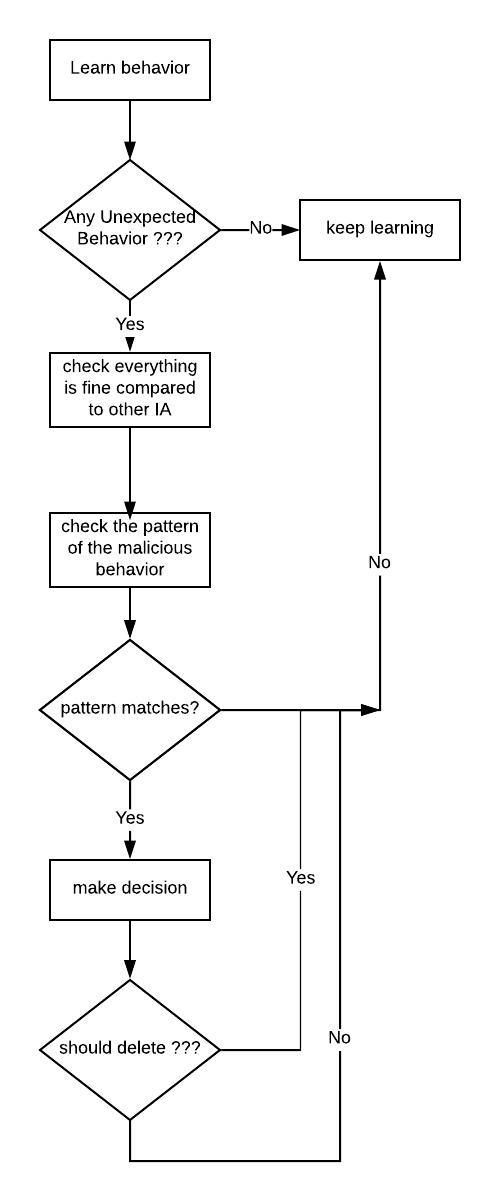
c) Check if all the settings are okay or not for that malicious behavior.

3. Then Neural Nets will check the pattern of that malicious behavior.

4. If the pattern matches with any other malicious behavior the expert system will give a decision this behavior should be delete or not .

5. If it won’t match with any pattern but it affects the system then the machine will learn about it and update its perception for the behavior.

**WORK FLOWCHART**

****

**EXPECTED OUTCOME**

Organisations face millions of threats each day, so it would be impossible for threat researchers to analyse and categorise them all. As each threat is analysed by the machine, it learns and improves. This not only helps protect organisations now, but compiles this valuable data for use in predictive analytics .However, just staying ahead of the hackers and the threats they pose is not enough to protect organisations as the new vulnerabilities and new devices that come online will make this more and more difficult. The continued and enhanced standardisation on data formats and communication standards is crucial to this effort. Once data flows and formats are clearly defined, not just technically but also semantically, machine learning systems will be far better placed to effectively police the operations of such systems.

**LIMITATIONS**

AI is by no means a cyber security panacea. When pitted directly against a human opponent, with clear circumvention goals, AI can be defeated. This doesn’t mean we shouldn’t use AI, it means we should understand its limitations. AI cannot be left to its own devices. It needs human interaction and “training” This hybrid approach already has proven itself to be a valuable asset in IT departments because it works efficiently alongside threat researchers.in AI-speak to continue to learn and improve, correcting for false positives and cyber criminal innovations.

**REFERENCES**

[1] Hal Lonas, CTO of ***[Webroot](https://www.webroot.com/gb/en" \t "_blank)*** , “The role of AI in Cyber Security”.

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

[3] E. Herrero, M. Corchado, A. Pellicer, A. Abraham, “Hybrid multi agent-neural NIDS with MV”.

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

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

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

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

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

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

[10] 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.

[11] 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.

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