ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Applications of Artificial Intelligence in Cyber Security

[1] Dr. Sunil Bhutada,[2]Preeti Bhutada
[1] Professor, Department of Information Technology, Sreenidhi Institute of Science and Technology
[2]Faculty, Front Office, Shri Shakti College of Hotel Management, Hyderabad

Abstract: In this era when the technology has come so far with a tremendous advancement in internet of things and connected devices, the experts of Cyber Security are facing a lot of issues. They need all the support that they can get to help them prevent the cyber-attacks and security breaches The organizations being more connected than ever is leading to heavy traffic, increase in security attack vectors, breaches in security and a lot more threats in the cyber are that is becoming more and more difficult to handle by humans alone. Developing a software system with standard logic for effectively defending against the growing cyber-attacks is however bothersome. On the other hand, the problems of cyber security can be efficiently resolved using the strategies involving AI.

Index Terms— Artificial Intelligence, Cyber-Security, Expert System, Intelligent Agent, Neural Nets.

I. INTRODUCTION

The incorporation of Artificial Intelligence into security systems can be used to reduce the ever increasing threats of cyber security that is being faced by the global businesses. Across the industries applications using Machine learning as well as artificial intelligence (AI) are broadly being used all the more as data collection, storage capabilities and computing power are increasing. In real time, the huge amount of data is difficult to be handled by humans. With the help of machine learning as well as Artificial Intelligence, the huge amount of data can probably be reduced down in milliseconds, as a result of which the enterprise can easily identify also recover from threat. Clearly barrier against savvy digital weapons can be accomplished just by insightful programming, and occasions of the most recent two years have indicated quickly expanding knowledge of malware and digital weapons.

II. ARTIFICIAL INTELLIGENCE

Initially Computer Security and Artificial Intelligence were considered to be two separate entities. To decrease human work, AI researchers were keen on creating programs, while security experts were attempting to fix the leakage of data. Over the time, the two fields have developed to be closer, as the attacks have focused to mimic the authentic execution, at the human client level as well as bring down system levels. CAPTCHAs can be considered a great example as a combination of AI and Security. In CAPTCHA, the client is to type the letters of a contorted picture, or letters or digits that are further in an obscured sequence that shows up on the screen. Enhancements in automated pattern recognition programming, which can be thought to be sensible progress in AI innovation, could spur the field towards more refined pattern recognition. Along these lines, during the time spent attempting to secure resources, for example, online ticket reservations, the business security market is in a way empowering progresses in AI. AI causes us in rapidly distinguishing and dissecting new endeavors and shortcomings to help moderate further attacks and is an essential piece of our answers. AI strategies are the way to Intrusion location and make it conceivable to react even to unidentified dangers. AI frameworks that are planned to learn and adjust, and are capable of recognizing even the slightest changes in the settings, can act considerably prior – and in view of tremendous trove of information – than people with regards to getting a handle on likewise novel kinds of digital attacks. It is for the most part acknowledged that AI can be considered in two different means: as a science that has developed for attempting to find the embodiment of knowledge and growing for the most part intelligent machines, or science giving techniques to taking care of complex issues that can't be settled without applying some insight like, for example, playing great chess or settling on right choices in view of a lot of information. Countless methodologies have been produced in the AI field for taking care of difficult issues that require insight from the human viewpoint. Some of these strategies have achieved a phase of development where exact algorithms exist that depend on these techniques. A few techniques have even

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

turned out to be so generally realized that they are not considered having a place with AI any more, rather we have categorized them. We layout these classes here, and we offer references to the utilization of particular strategies in cyber security.

A. Expert Systems

Expert systems are irrefutably the most popular AI tools. Expert system is programming for discovering answers to inquiries in some application area displayed either by user or by another product. It can be straightforwardly utilized for choice help, e.g. medical diagnosis, in accounts or in the internet. There is an extraordinary assortment of expert systems from little specialized diagnostic systems to substantially large and refined hybrid systems to take care of complex issues. Theoretically, expert system incorporates a knowledge base, where expert information about a particular application area is kept. Other than knowledge base, it incorporates an inference engine for inferring answers in light of this information and, conceivably, extra information about a circumstance. Discharge knowledge base and inference engine are as one called expert system shell - it must be loaded with information, before it can be utilized. Expert system shell must be bolstered by programming for including information in the knowledge base, and it can be reached out with programs for client collaborations, and with different projects that might be utilized as a part of hybrid expert systems. Building up an expert system implies, in the first place, choice/adjustment of an expert system shell and, secondly gaining expert information and filling the knowledge base with the information. The step two is by a wide margin more complex and tedious than the first. There are numerous tools for creating expert systems. When all is said and done, a device incorporates an expert system shell and has likewise a usefulness for adding information to the knowledge repository. Expert systems can have additional usefulness for reenactment, for making estimations and so on. There are a wide range of information display forms in expert systems, the most well-known is a rule based portrayal. However, the convenience of an expert system depends fundamentally on the nature of information in the knowledge base of the expert system, and less on the internal representation of the information portrayal. This leads one to the information procurement issue that is significant in developing real time applications. Case of a CD expert system is one for security arranging.

This expert system encourages impressively choice of safety efforts, and gives direction to ideal use of restricted assets. The Security expert system takes after an arrangement of ventures to battle cyber-attacks. It checks the procedure with the knowledge base in the event that it is a known process then disregard it, else the framework ought to end the procedure. In the event that there is no such procedure in knowledge base, the expert system uses inference engine algorithms and finds the machine state. The machine state has been ordered into three; sheltered, direct and extreme. As per the machine state the framework cautions the administrator/user and the inference has been bolster to Knowledge base.

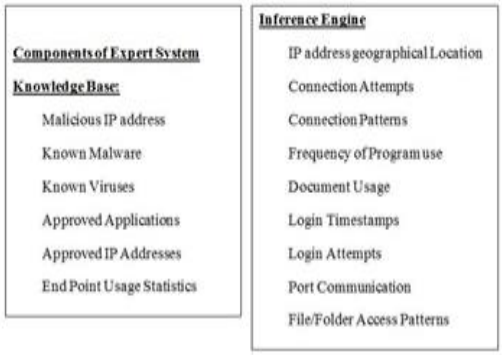

Figure 1: Security Expert System Components

B. Neural Nets

Neural nets is otherwise called deep learning is a propelled branch of AI. It is enlivened by the elements of the human mind. Our mind has large number of neurons, which are to a great extent general purpose and independent of domain, they can take in any kind of information. An artificial neuron (Perceptron) was made in 1957 by Frank Rosenblatt which laid the route for neural systems. These perceptron can master and handle interesting issues by consolidating with other perceptron. They learn without any external help to recognize the entity using which they are trained by learning and handling the high level raw information, as our mind takes in its own from the raw information utilizing our sensory organ's sources of info. At the point when this deep learning is connected to cyber security, the framework can distinguish whether a document is malicious or legitimate without any intervention by humans. This procedure uncovers solid outcomes in recognizing the malware, contrasted with classical machine learning. The accomplishment of neural nets in cyber security is their faster outcomes when upheld in graphical processors or equipment. Neural nets can empower the exact recognition of new malware dangers and fill in the holes that that leave organizations presented to attacks.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

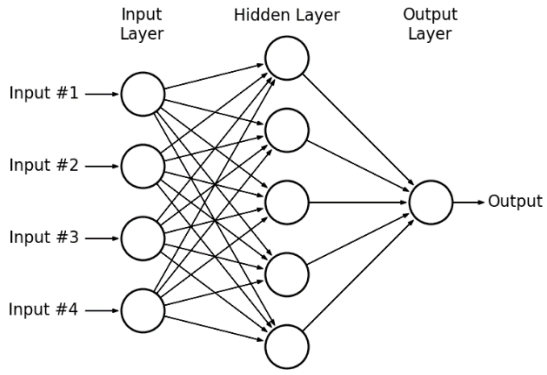

Figure 2: Neural Nets

C. Intelligent Agents

Intelligent agent (IA) is an autonomous entity which sees through sensors and follows up on a domain utilizing actuators and coordinates its action towards accomplishing objectives. Intelligent agent may likewise learn or utilize information to accomplish their objectives. They can adjust to real time, learn new things rapidly through communication with environment, and have memory based model storage and recovery capacities. Intelligent agent is created in protection against Distributed Denial of Service (DDoS) attacks. On the off chance that if there is any legitimate and business issue, it ought to be reasonable to build up a "Digital police" which has portable intelligent agents. For this we should actualize the foundation to help the quality and interaction between the intelligent agents.

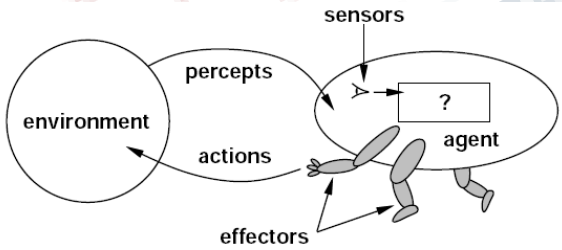

Figure 3: Intelligent Agents

D. Search

Search is a widespread strategy for critical thinking that can be connected in all situations when no different strategies for critical thinking are appropriate. Individuals apply search in their regular day to day existence continually, without focusing on it. Next to no must be known keeping in mind the end goal to apply some broad pursuit calculation in the formal setting of the inquiry issue: one must have the capacity to produce applicants of arrangements, and a system must be accessible for choosing whether a proposed competitor fulfills the necessities for an answer. Nonetheless, if extra learning can be manipulated to manage the search, at that point the proficiency of inquiry can be radically moved forward. Search is available in some way nearly in each intelliegnt program, and its proficiency is frequently basic to the execution of the entire program. An extraordinary assortment of search techniques have been created which consider the particular information about specific inquiry issues. Albeit numerous search techniques have been produced in AI, and they are generally utilized as a part of numerous projects, it is rarely used in AI. For instance, dynamic writing computer programs is basically utilized as a part of taking care of ideal security issues, the inquiry is covered up in the product and it is unmistakable as an AI application. The αβ-search calculation, initially created for PC chess, is a usage of a by and large helpful thought of "isolate and vanquish" in critical thinking, and particularly in basic leadership when two foes are picking their most ideal activities. It utilizes the evaluations of negligibly ensured win and maximally conceivable misfortune. This empowers one frequently to overlook huge measure of choices and significantly to accelerate the search.

E. Learning

Learning is enhancing an information system by expanding or revamping its knowledge base or by enhancing the inference machine. This is a standout amongst the most fascinating issues of counterfeit consciousness that is under concentrated examination. Machine learning contains computational techniques for obtaining new information, new abilities and better approaches to arrange existing information. Issues of learning change extraordinarily by their unpredictability from basic parametric learning which implies learning estimations of a few parameters, to entangled types of symbolic learning, for case, learning of ideas, sentence structures, capacities, notwithstanding learning of conduct . AI gives techniques to both - directed getting the hang of (learning with an instructor) and unsupervised learning. The last is particularly valuable on account of quality of expansive measure of information, and this is basic in digital guard where huge logs can be gathered. Data mining has initially become out of unsupervised learning in AI. Unsupervised learning can be a usefulness of neural nets, specifically, of self-sorting out maps. A recognized class of learning strategies is constituted by parallel learning calculations that are appropriate for execution on parallel equipment. These learning strategies are spoken

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

to by genetic algorithms and neural nets. Genetic algorithms as well as fuzzy logic, for example, have been utilized as a part of danger identification systems depicted.

F. Constraint tackling

Constraint solving is a method created in AI for discovering answers for issues that are introduced by giving an arrangement of imperatives on the arrangement, e.g. sensible proclamations, tables, conditions, imbalances. An answer of an issue is a gathering (a tuple) of qualities that fulfill all imperatives. As a matter of fact, there are a wide range of requirement tackling strategies, contingent upon the idea of imperatives (for instance, limitations on limited sets, useful limitations, and levelheaded trees). On an exceptionally unique level, any issue can be introduced as an imperative fulfillment issue. Specifically, numerous arranging issues can be exhibited as requirement fulfillment issues. These issues are hard to illuminate as a result of expansive measure of hunt required by and large. All requirement tackling techniques are gone for confining the inquiry by considering particular data about the specific class of issues. Requirement fathoming can be utilized as a part of circumstance investigation and choice help in blend with rationale programming.

III. AI TECHNIQUE ADVANTAGES

We can utilize AI in different ways for cyber security. In future, we may have most clever frameworks than these methods. Indeed, even the attackers/ intruders will likewise utilize the AI for attacks. Clearly, the new advancements in information comprehension outline and dealing with what is more in machine learning will extraordinarily improve the digital security capacity of frameworks that may utilize them. The summation of different methods examined in this paper is appeared in the figure below

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)

Figure 4: Advantages of AI techniques

IV. DISADVANTAGES IN INELLIGENT CYBER SECURITY

When arranging the future research, advancement and utilization of AI strategies in CD, one needs to recognize the prompt objectives and long haul points of view. There are various AI strategies instantly pertinent in CD, and there are prompt CD issues that require more keen arrangements than have been actualized at exhibit. Up to this point we have talked about these current quick applications. Later on, one can see promising viewpoints of the use of totally new standards of learning taking care of in circumstance administration and basic leadership. These standards incorporate presentation of a particular and various leveled learning design in the basic leadership programming. A testing application region is the learning administration for net driven fighting. Just computerized information administration can ensure quick circumstance appraisal that gives a choice prevalence over pioneers and chiefs on any C2 level. For instance, the paper depicts a thought of the various leveled and secluded learning engineering in the Joint Command and Control Information System of the Bundeswehr. Expert systems are now being utilized as a part of numerous applications, in some cases covered up inside an application, as in the safety efforts arranging programming. In any case, expert systems can get more extensive application, if expansive learning bases will be produced. This will require impressive interest in learning procurement, and improvement of substantial secluded information bases. Additionally further advancement of the expert framework innovation will be required: measured quality must be presented in the expert framework apparatuses, and various leveled learning bases must be utilized. Considering a more far off future - at any rate a few decades ahead, maybe we ought not to confine us to the "restricted AI". A few people are persuaded that the fantastic objective of the AI - improvement of counterfeit general insight - AGI can be come to amidst the present century. The primary meeting on AGI was held in 2008 at the University of Memphis. The Singularity Institute for Artificial Intelligence (SIAI), established in 2000, cautions specialists of a risk that exponentially speedier advancement of insight in PCs may happen. This improvement may prompt Singularity, portrayed as takes after: "The Singularity is the innovative making of quicker witted than-human knowledge. There are a few advances that are frequently said as traveling toward this path. The most normally said is presumably Artificial Intelligence, however there are others - a few distinct advancements which, in the event that they achieved a

limit level of refinement, would empower the making of more astute than-human knowledge. ... A future that contains more brilliant than-human personalities is truly unique in a way that goes past the standard dreams of a future loaded with greater and better devices." A futurist Ray Kurtzwell has extrapolated the advancement to think of Singularity in 2045 [39]. One need not to trust in the Singularity danger, but rather the quick improvement of data innovation will empower one to incorporate extensively better insight with programming in coming years. (Consider the current amazing execution of IBM-s Watson program.) Independently of whether the AGI is accessible or Singularity comes, it is critical to be able to utilize preferable AI in digital safeguard over the wrongdoers have it.

IV. CONCLUSION

In the current situation due to rising advancement in malware and cyber-attacks, Intelligent Security System is required. Appeared differently in relation to contemporary cyber security solutions, AI methods are robust and more flexible; as a result expanding security execution and better defense system from an increasing number of advance cyber threats. Despite the intense change that AI has passed on to the area of cyber security, related systems are not yet prepared to adjust totally and thus to changes in their condition. In spite of the fact that we have numerous advantages when we utilize AI procedures for cyber security, AI isn't the main panacea for security. At the point when a human opponent with an unmistakable circumvention goal attacks the intelligent security the framework will fail. This doesn't imply that we cannot utilize AI methods, but rather we should know its restrictions and utilize it properly. AI needs ceaseless human collaboration and training. Alongside the threat researchers this approach of AI with Cyber Security has proven to work efficiently.

REFERENCES

[1] E. Tyugu. Algorithms and Architectures of Artificial Intelligence.IOS Press. 2007.
[2] NabaSuroor 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.
[3] D. Anderson, T. Frivold, A. Valdes. Next-generation intrusion detection expert system (NIDES).
[4] F. Rosenblatt. The Perceptron -- a perceiving and recognizing automaton. Report 85-460-1, Cornell natural philosophy Laboratory, 1957.
[5] I. Bratko. logic programming Programming for engineering. Addison-Wesley, 2001 (thirdedition).http://ieeexplore.ieee.org/document/4639011
[6]https://business.f-secure.com/whats-the-deal-with-artificiai-intelligence-in-cyber-security
[7]http://www.information-age.com/role-ai-cyber-security-123465795/
[8] B. Mayo, E. Tyugu, J. Penjam. Constraint Programming. Alignment ASI Series, v. 131, Springer-Verlag. 1994.
[9] F. Barika, K. Hadjar, and N. El-Kadhi, "ANN for mobile IDS solution," in Security and Management.
[10] TF. Lunt, R. Jagannathan. A Prototype Real-Time Intrusion-Detection Expert System.Proc.
[11] B. Iftikhar, A. S. Alghamdi, "Application of artificial neural network within the detection of dos attacks," in SIN '09: Proceedings of the ordinal international conference on Security of knowledge and networks. New York, NY, USA: ACM, 2009, pp. 229–234.
[12] P. Norvig, S. Russell. Artificial Intelligence: fashionable Approach. tiro Hall, 2000.
[13] http://en.wikipedia.org/wiki/Expert_system. accomplished System. Wikipedia
[14] P. Salvador et al. Framework for Zombie Detection Using Neural Networks. In: Fourth International Conference on Internet Monitoring and Protection ICIMP-09, 2009.
[15] M. Shankarapani, K. Kancherla, S. Ramammoorthy, R. Movva, and S. Mukkamala. Kernel Machines for Malware Classification and Similarity Analysis. WCCI 2010 IEEE World Congress on Computational Intelligence. Barcelona, Spain, 2010, pp. 2504 – 2509.
[16] 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.
[17] http://en.wikipedia.org/wiki/Expert_system. Expert System. Wikipedia.
[18] J. Kivimaa, A. Ojamaa, E. Tyugu. Graded Security Expert System. Lecture Notes in Computer Science, v. 5508. Springer, 2009, 279-286.
[19] D. Anderson, T. Frivold, A. Valdes. Next-generation intrusion detection expert system (NIDES). Technical Report SRI-CSL-95-07, SRI International, Computer Science Lab (1995).
[20] TF. Lunt, R. Jagannathan. A Prototype Real-Time Intrusion-Detection Expert System. Proc. IEEE Symposium on Security and Privacy, 1988, p. 59.
[21] I. Kotenko, A. Ulanov. Multi-Agent Framework fo Simulation of Adaptive Cooperative Defense Against

Internet Attacks. In: International Workshop on Autonomous Intelligent Systems: Agents and Data Mining. LNCS, Springer, v. 4476.

[22] I. Kotenko, A. Konovalov, A.Shorov. Agent-Based modeling and Simulation of Botnets and Botnet Defence. In: C. Czosseck, K. Podins (eds.). Proc. Conference on Cyber Conflict. CCD COE Publications, Tallinn, Estonia, 2010.

[23] B. Stahl, D. Elizondo, M. Carroll-Mayer, Y. Zheng, K. Wakunuma. Ethical and Legal Issues of the Use of Computational Intelligence Techniques in Computer Security and Computer Forensics. In: WCCI 2010 IEEE World Congress on Computational Intelligence, Barcelona, Spain. 2010, pp. 1822 – 1829.

[24] E. Herrero, M. Corchado, A. Pellicer, A. Abraham, "Hybrid multi agent-neural network intrusion detection with mobile visualization," Innovations in Hybrid Intelligent Systems, vol. 44, 2007, pp. 320–328.

[25] V. Chatzigiannakis, G. Androulidakis, B. Maglaris. A Distributed Intrusion Detection Prototype Using Security Agents. HP OpenView University Association, 2004.

[26] J. Kivimaa, A. Ojamaa, E. Tyugu. Pareto-Optimal Situation Analysis for Selection of Security Measures. Proc. MilCom, 2008.