IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ARTIFICIAL INTELLIGENCE: THE NEW AGE OF CYBERSECURITY

[1]Padma Rajani, [2]Sangeeta Adike, [3]S. G. K. Abhishek

[1]Associate Professor, [2]Student, [3]Student
[1]CSE Department,
[1]Guru Nanak Institutions Technical Campus, Hyderabad, India

Abstract: Technology has come a long way with rapid advancements on the Internet, IoT (Internet of Things), and other such connecting Technologies. Currently, scientists and experts alike, are facing many issues to prevent cyber-attacks and data breaches. Corporate enterprises and individuals are more connected than ever before, thus leading to high amounts of network traffic. As a result, detecting and preventing security attacks is getting more and more difficult to be handled by us humans alone. Hence, Artificially Intelligent Software models could be developed to defend against such cyber-attacks and therefore, can also improve cybersecurity using such strategies. This paper discusses the implementations and some plausible areas where AI can be implemented in the field of Cybersecurity.

***Index Terms* - Artificial Intelligence, Cyber-Security, Expert System, Intelligent Agent, Neural Nets, Constraint Tackling.**

I. INTRODUCTION

Artificial Intelligence (AI) can be incorporated into security systems to reduce the rapidly evolving and rising threats of cybersecurity that are being faced by both small and large-scale businesses. Machine Learning (ML) along with Artificial Intelligence is extensively being used in industrial applications as the rate of data collection, storage capabilities and computing power has day-by-day gone on a rise. Such huge amounts of collected data can be cumbersome for humans to handle. With the help of AI and ML, enormous data can be depreciated within milliseconds, due to which, enterprises can easily identify and recover from any threats. Application of Network Centric Warfare (NCW) makes cyber incidents especially dangerous, and changes in cyber defense are urgently required [1]. Intuitive programming and the expanding knowledge of malware and digital weapons archived for a couple of years can help in achieving a form of barricade against such malicious attacks.

II. ARTIFICIAL INTELLIGENCE

Computer Science and Artificial Intelligence were initially thought of as separate subjects. To minimize human labour, AI researchers were driven to create programs, while security experts were sorting out ways to prevent data leakage. Over time, these two fields have worked hand-in-hand, as attacks have taken a more authentic approach of execution, at the human client level while also tricking security systems. CAPTCHAs are considered to be a good example of Security with the help of AI. Here, the client is required to enter a particular sequence of letters from a distorted image, or simply letters and/or numbers that are viewed in an unusual pattern on a computer screen. Improvements in generated pattern recognition programming, which is seen as an innovation in the field of AI, could push the technology towards a more polished pattern recognition system.

As such programs are being implemented into businesses to improve the security of data that they handle (Ex. Online Payment Gateways), they are consequently causing AI to progress. AI helps in rapidly distinguishing and analysing new efforts and shortcomings to assist in further moderating attacks and can be an essential solution for cybersecurity. AI strategies are ways of intrusion location and can efficiently and effectively react to unseen dangers that were not initially possible. There are frameworks that are trained to learn and adjust, and capable of taking into account even the subtlest changes in the software. These AI frameworks can perform considerably better and look deeper into the program/system than people who are responsible for looking into typical kinds of digital attacks. Therefore, we can consider AI to be the following:

- A Science or Study that has developed by attempting to find solutions from existing knowledge or growing mostly intelligent machines, or
- Science that gives techniques and methods to look after complex problems that can't be solved without providing any form of insight like, for playing a game of Go, or for taking the right decisions in accordance with a given set of information. [2]

There have been numerous methodologies produced in AI for solving such difficult issues that require a human perspective. There have also been instances during the development of AI strategies where definitive algorithms are available that depend on these techniques. A few of them could be traced into an algorithm due to which, they are not termed as an AI strategy, but have simply been categorized. We have discussed the classes below and also offer references towards utilizing these in cyber security.

2.1 Expert Systems:

Expert systems are undeniably one of the most popular AI tools. An Expert system is a programming methodology for finding answers to queries in some application areas that are displayed either by a user or by other systems. It can plainly be used for choice help, e.g.: Internet, Accounts, or in Medical Diagnosis. There is an astonishing assortment of these systems from small specialized diagnostic systems to considerably large and hybrid systems to take care of complicated problems. In theory, Expert systems incorporate a knowledge base, where expert information about a particular application area is kept.

In addition to a knowledge base, it also incorporates an inference engine to infer answers with reference to this information and the extra information about a circumstance.

Discharge knowledge base and inference engine are collectively called an "Expert system Shell" - it must be loaded with information before it is being utilized. Expert systems should be backed by programming for adding information to the knowledge base, and it can be reached out for programs for client collaboration, along with an array of different projects that may be utilized as a part of hybrid expert systems. To build an expert system we require, firstly, adjustment/choice of an expert system shell and, secondly gaining expert information and populating the knowledge base with the added information. The second step is built up by a wide margin more complex and tedious than the first.

There are many tools for creating expert systems. When all is taken care of, the device then incorporates an expert system shell and likewise useful for adding information to the knowledge repository. These systems may also have additional usefulness for re-enactment, for making estimations and many more. There are a vast amount of information display forms in expert systems, rule based portrayal is the most known. [However, the convenience depends basically upon the nature of information in the knowledge base of the expert system, and less on the internal representation of the portrayal of information. This leads to the information procurement problem that is most noticeable in real time application development. For instance, a Cyber Defence (CD) expert system is the one used for security arranging.[17].

This expert system encourages an impressive choice of safety efforts, and gives ways to ideal use of restricted assets. The security expert system takes a look at an arrangement of ventures to battle cyber-attacks. It verifies the procedure in the knowledge base. If it is a known process, it disregards it. In the event where there is no such procedure in the knowledge base, this expert system uses the algorithms of the inference engine and finds the machine state. This machine state is ordered into three:

1. Extreme
2. Direct
3. Sheltered

According to the state of the machine, the framework cautions the user or administrator that the inference has been appended to the knowledge base.

Knowledge Base:
Malicious IP Address
Known Malware
Known Viruses
Approved Applications
Approved IP Addresses
End Point Usage Statistics

Inference Engine:
IP Address Geological Location
Connection Attempts
Connection Patterns
Frequency of Program Use
Document Usage
Login Timestamps
Login Attempts
Post Communication
File/Folder Access Patterns

Fig.1: Components of Security Expert System [4]

2.2 Neural Nets

Neural Nets, also called Deep Learning, is a propelled branch of Artificial Intelligence. It is made more interesting by the human mind element. Our mind consists of a large number of neurons, which are independent of each other and can take in and process any kind of information. A Perceptron (artificial neuron) was coined by Frank Rosenblatt in 1957, [3] which led to the concept for neural systems. These perceptrons can handle and adept to any issue by connecting with other perceptrons. They learn without any intervention, without any help externally to identify the entity with which they are trained by learning and handling the high level raw information, as our mind takes its own from the raw information acquired by our sense organs. At the point when these neural nets are connected to cyber security, the AI framework can decide whether that document is legitimate or not without any human intervention. This procedure uncovers beneficial outcomes in identifying malware, as opposed to classical machine learning. The achievement of neural nets in cyber security is their faster outcomes when upheld in graphical equipment.

Neural nets can authorize the exact identification of new malware dangers and fill in the holes that leave organizations presented to attacks. Neural nets are well applicable in intrusion detection and intrusion prevention[5,6,7,8,9]. There have been proposals to use them in DoS detection[10], computer worm detection[11], spam detection [12], zombie detection[13], malware classification[14], and in forensic investigations[15]. Intelligent Agents can easily adjust with the real time environment, and have memory.

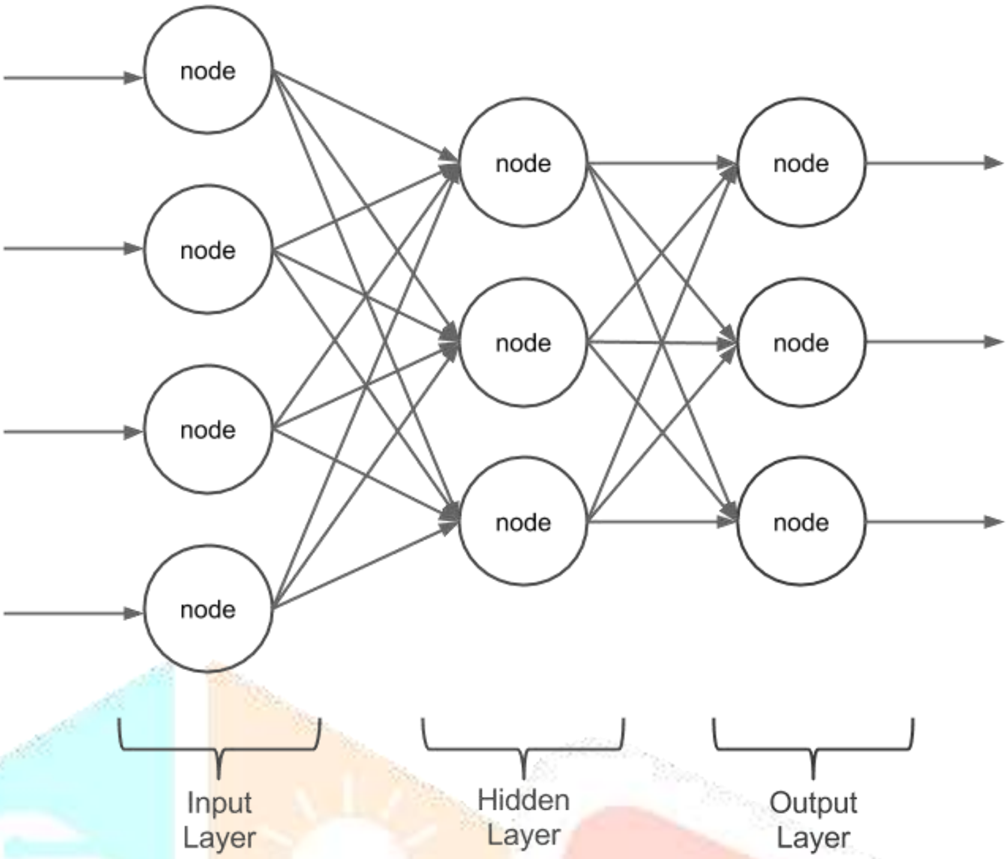

Fig.2: An example of Neural Nets [16]

2.3 Intelligent Agents

Intelligent agent (IA) is an independent entity which sees through sensors and follows up by using actuators and coordinates its action towards the desired objectives. Moreover, they can learn or make use of information to accomplish their goal. based model storage and recovery capabilities. Intelligent Agents are created for protection against DDoS (Distributed Denial of Service) attacks. In case of any legitimate business issue,[18] the IA creates a “Digital Police” which has portable Intelligent Agents. For this to take place, we should enable the necessities for good quality and good interaction between Intelligent Agents.

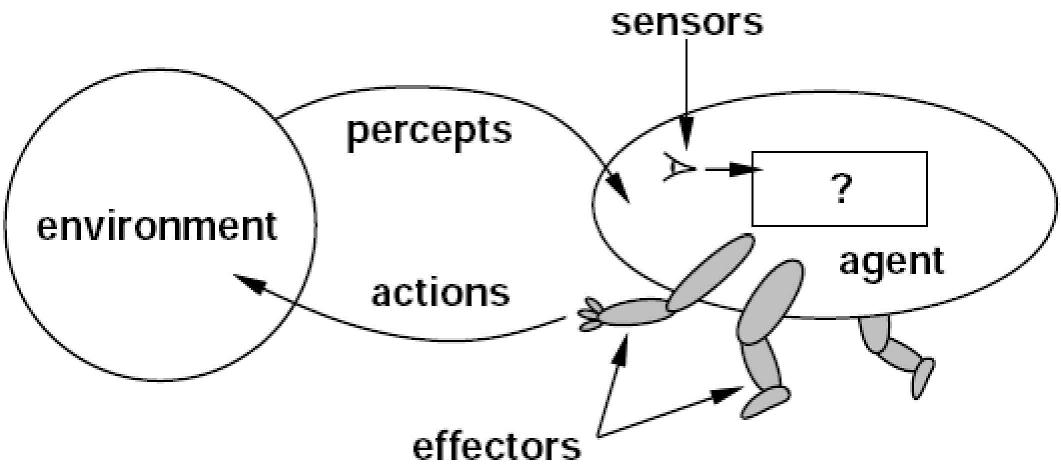

Fig.3: Simple Working of an Intelligent Agent [19]

2.4 Search

This is an extensive strategy for critical thinking that can be implemented in all situations when no other strategy for critical thinking is suitable. We make use of Search regularly, without any notice. We must also keep in mind the end goal to apply some broad pursuit calculation in the setting of the inquiry issue: one must have the capability to produce applicants of arrangements, and a system must be accessible to choose whether the presented competitor meets the requirements for the answer. Nevertheless, if extra knowledge can be extracted to direct the search, then we can notice a drastic improvement in the efficiency of the search taking place. In every intelligent program we can find this strategy in some form, and the criticality of the whole program depends on its efficiency.

Many search methods have been developed which depend on the particular knowledge about specific search problems. Even though there are many search methods developed and they are widely used in programs, Search is very rarely considered as a usage of AI. For example, dynamic programming is essentially used in solving optimal security problems, the search is hidden in the software and it is not visible as an AI application [20,21]. Games make use or searches like αβ-search, minimax search and stochastic search and are useful in cyber-defence decision-making. The αβ-search algorithm makes use of the “divide and conquer” approach and was basically developed for computer chess, especially in the decision-making when two opponents are selecting the best possible move. This quickens the search as a large number of options are overlooked because it approximates the maximally feasible failure over the minimum feasible wins.

2.5 Learning

Learning is enhancing an information system by expanding its knowledge base or by enhancing the inference machine. [22]. This is a standout amongst the most familiar problems of counterfeit consciousness that is under concentrated examination. Machine learning consists of computational methods for gaining new knowledge, skills and new ways to organize with the existing knowledge. Problems of learning vary by their complexity from complicated forms of symbolic learning and simple parametric learning, e.g., functions, grammar, etc[23].

Supervised learning and Unsupervised learning are provided with different methods through AI. This is specifically used in the presence of huge amounts of data, and this is very common in cyber defence where collections of logs are present. Data mining has been originally developed off unsupervised learning in AI. In particular, unsupervised learning could be a part of deep learning, especially the self-organizing maps [9,15,24,25].

Parallel learning algorithms help constitute a notable range of learning methods that benefit from parallel hardware execution. Genetic algorithms and neural nets are used to represent such methods. Genetic algorithms and fuzzy logic has been, for instance, used in threat detection systems [26].

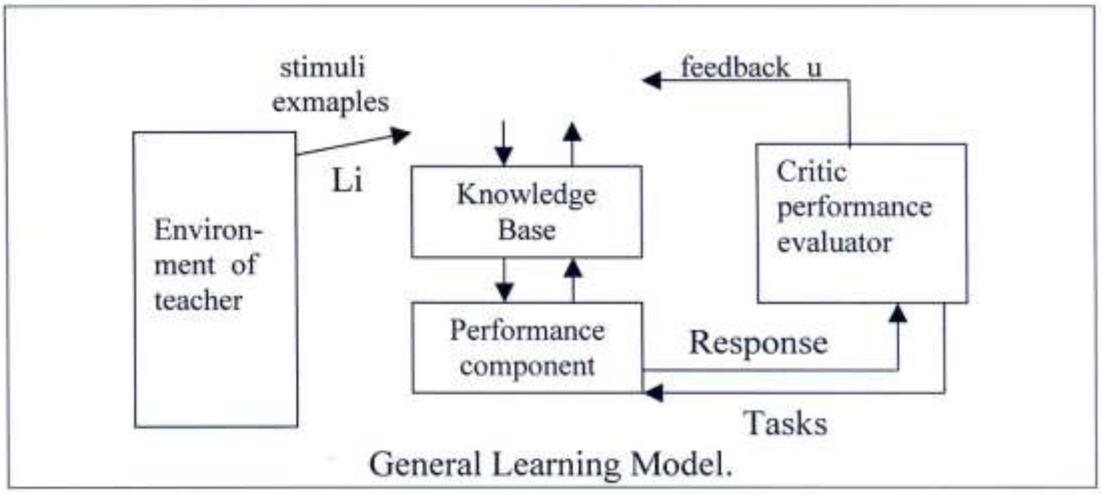

Fig.4: General Learning Model

2.6 Constraint Tackling

Constraint solving is a method that is created in AI for discovering answers for the problems that are introduced by giving an arrangement of imperatives on the arrangement, E.g. Tables, conditions, imbalances [2,27]. An answer to any problem is a tuple or gathering of qualities that fulfil all imperatives. There are a wide range of requirements tackling strategies, contingent upon the idea of imperatives. On a unique level of expectation, any problem can be introduced as an imperative fulfilment issue.

In particular, numerous arranging issues can be exhibited as requirement fulfilment issues. These issues are hard to illustrate as a result of the expansive measure of hunt required by and large. All required 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 circumstances investigation and choice help in blend with rationale programming. Constraint solving can be used in situation analysis and decision support in combination with logic programming [28,29].

III. BENEFITS OF ARTIFICIAL INTELLIGENCE CYBERSECURITY STRATEGIES

AI can be incorporated in many different ways in cybersecurity. We may even have the most intelligent frameworks in the future in contrast to the above mentioned techniques. In fact, even attackers and intruders could use AI to execute their attacks. Certainly, improvements in the capacity of digital security of frameworks can be perceivable as there are new developments in the outline of information comprehension and dealing more into machine learning. The advantages of some of the AI strategies discussed before are given below:

Table 1 Advantages of AI Strategies

AI Techniques	Usage
Application of Intelligent Agent	• Proactive & Reactive • Agent Communication Language • Mobility • Defence against DDoS
Application of Neural Nets	• For Intrusion Detection and Prevention Systems • Very High Speed of Operation • For DDoS Detection • For Forensics Investigation • Worm Detection
Application of Expert Systems	• For Detection Support • For Network Intrusion • Knowledge Base • Inference Engine
Application of Learning	• Machine Learning • Supervised Learning & Unsupervised Learning • Malware & Intrusion Detection • Self-Organising Maps (SOMS)

IV. CHALLENGES OF ARTRIFICIAL INTELIIGENCE CYBERSECURITY STRATEGIES

One needs to interpret the immediate objectives and sustainable viewpoints, while making arrangements for future analysis and also taking in mind, improvements and usage of these AI strategies in Cyber Defense (CD). There is an array of AI strategies, straight away relevant to CD, and there are also many motivational concerns regarding CD that demand more clever solutions that are presently being implemented as we discuss. Thus far, we have reviewed a few of these available applications.

Going forward, we could see newer standards of information handling in situation management and decision-making which could show encouraging standpoints. One such challenging implementation is the knowledge management of net centric warfare [32]. Guaranteed swift status assessments can take place with the help of spontaneous Knowledge Management which gives Decision makers and leaders supremacy on any C2 Level.

Expert Systems can be concealed within an application and is used in many scenarios. Although, if knowledge bases are improvised, expert systems can be used at a wider scale. This obviously would require substantial capital for knowledge acquisition, and the making of enormous regulatable knowledge bases. Also, expert systems have to be further developed to incorporate modularity and hierarchy.

Several individuals believe that by the middle of this century, the development of an Artificial General Intelligence (AGI) is possible. The Singularity Institute for Artificial Intelligence (SIAI) (est. 2002), has alerted experts that rapid advancement in computer intelligence can take place. This may lead to Singularity [33]. Ray Kurtzwell, a futurist, has come up with the means to devise a singularity by 2045 [34]. Whether it be the development of AGI or the creation of Singularity, it is of utmost importance to have the capacity to use improved AI in cyber defense rather than the intruders having it.

V. CONCLUSION

In the present situation where sophisticated and Intelligent Security Systems are being implemented due to growing advancements in malware and cyber-threats. DDoS Mitigation experience has demonstrated that defense against massive attacks can be achieved with limited resources. A publication analysis also shows that research into neural nets has brought fruitful AI results when applied in CD. There is an urgent need for intelligent cyber defense strategies in areas such as but not limited to: Knowledge Management, Situation Awareness, etc. In such an instance, Expert Systems are more favorable.

It is uncertain how quickly the growth of General Artificial Intelligence is further down the road. But there may be a new class of AI that may be used by criminals. Hence, we must be prepared with various developments in knowledge interpretation, representation and handling along with machine learning to significantly strengthen Cyber Defense capability of systems.

REFERENCES

[1] R. A. Poell, P. C. Szklarz. R3 – Getting the Right Information to the Right People, Right in Time. Exploiting the NATO NEC. In: M.-Amanowicz. Concepts and Implementations for Innovative Military Communications and Information Technologies. Military University of Technology Publisher, Warsaw, 2010.

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

[3] F. Rosenblatt. The Perceptron -- a perceiving and recognizing automaton. Report 85460-1, Cornell Aeronautical Laboratory, 1957.

[4] http://irjcs.com/volumes/vol4/iss09/05.SISPCS10092.pdf

[5] J. Bai, Y. Wu, G. Wang, S. X. Yang, andetworks - ISNN 2006, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, May 2006, pp. 255–260.

[6] F. Barika, K. Hadjar, and N. El-Kadhi, "Artificial neural network for mobile IDS solution," in Security and Management, 2009, pp. 271–277.

[7] D. A. Bitter, T. Elizondo, Watson. Application of Artificial Neural Networks and Related Techniques to Intrusion Detection. WCCI 2010 IEEE World Congress on Computational Intelligence. July, 18-23, 2010 - CCIB, Barcelona, Spain, 2010, pp. 949 – 954.

[8] 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," International Journal of Computational Intelligence Research, vol. 3, no. 1, 2007, pp. 6–10.

[9] L. DeLooze, Attack Characterization and Intrusion Detection using an Ensemble of Self-Organizing Maps, Proceedings of the IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, 2006.

[10] B. Iftikhar, A. S. Alghamdi, "Application of artificial neural network in detection of dos attacks," in SIN '09: Proceedings of the 2nd international conference on Security of information and networks. New York, NY, USA: ACM, 2009, pp. 229–234.

[11] D. Stoepel, Z. Boger, R. Moskovitch, Y. Shahar, and Y. Elovici, "Application of artificial neural networks techniques to computer worm detection," in International Joint Conference on Neural Networks (IJCNN), 2006, pp. 2362–2369.

[12] C.-H. Wu, "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," Expert Systems with Applications, vol. 36, no. 3, Part 1, 2009, pp. 4321–4330.

[13] P. Salvador et al. Framework for Zombie Detection Using Neural Networks. In: Fourth International Conference on Internet Monitoring and Protection ICIMP-09, 2009.

[14] M. Shankar Pani, 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.

[15] 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.

[16] https://datadan.io/neural-net-with-go

[17] J. Kivimaa, A. Ojamaa, E. Tyugu. Graded Security Expert System. Lecture Notes in Computer Science, v. 5508. Springer, 2009, 279-286.

[18] 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.

[19] https://www.doc.ic.ac.uk/project/examples/2005/163/g0516334/index.html

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

[21] J. Kivimaa, A. Ojamaa, E. Tyugu. Managing Evolving Security Situations. MILCOM 2009: Unclassified Proceedings, Boston, MA. Piscataway, NJ: IEEE, 2009, pp. 1 - 7.

[22] P. Norvig, S. Russell. Artificial Intelligence: a Modern Approach. Prentice Hall, 2000.

[23] AK. Ghosh, C. Michael, M. Schatz. A Real-Time Intrusion Detection System Based on Learning Program Behavior. Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection, 2000, pp.93-109.

[24] 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, in Advances in Neural Networks. Lecture Notes in Computer Science. Springer, 2006, pp. 255–260.

[25] V. K. Pachghare, P. Kulkarni, D. M. Nikam. Intrusion Detection System using Self Organizing Maps. Proc. International Conference on Intelligent Agent & MultimediaAgent Systems, IAMA 2009.

[26] 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.

[27] B. Mayoh, E. Tyugu, J. Penjam. Constraint Programming. NATO ASI Series, v. 131, Springer Verlag. 1994.

[28] I. Bratko. PROLOG Programming for Artificial Intelligence. Addison-Wesley, 2001 (third edition).

[29] Xinming Ou. A logic-programming approach to network security analysis. PhD Thesis, Princeton University, 2005.

[30] https://artificialintelligence-notes.blogspot.com/2010/07/general-learning-model.html

[31] http://ijercse.com/specissue/aprilissue/38.pdf

[32] J. Kaster. Combined Knowledge Management and Workflow Management in C2 Systems – a user centered approach. Fraunhofer Institute for Communication, Information Processing and Ergonomics. Report ID # 197, 2009

[33] http://singinst.org/overview/whatisthesingularity/

[34] http://www.ted.com/webcast/archive/event/ibmwatson