Application of Artificial Intelligence for Securing Computer Networks

Arvind Kishanrao Rathod[1], Bhushan Shivajirao Kulkarni[2]

(Lecturer in Computer Engineering[1], Departmant of Computer Engineering[1])

(Lecturer in Elect. & Telecomm. Engineering[2], Dept. of Elect & Telecomm Engineering[2])

Government Polytechnic Jintur - 431509

Abstract: Artificial Intelligence is a revolutionary technology which the Computer industry is exploring, with the aim of introducing it into Computer networks and to provide new services, to secure Computer networks and to improve network efficiency by monitoring Computer networks and user experience. These Artificial Intelligence algorithms have been shown to demonstrate their respective capabilities to produce high performance accuracies in various Computer network securing applications.

Keywords: Computer Service Providers, Multi-Level Perceptron, clustering, Computational Intelligence, Hybrid Learning, Supervised Learning, Unsupervised Learning

Introduction: The Information Technology sector is diverse, running the gamut from standard voice service to internet-linked control systems of all critical infrastructures, It may be the most vulnerable to the increasing risk of cyber attack, this complex system runs the risk of significant disruption. Also today's Computer Networks Technology changes faster than ever with technologies such as 5G and internet of things (IoT) leading the way to increased speed and bandwidth, but also increased connectivity complexity. Through these ongoing changes and migrations to the next generation of Computers, Computers service providers (CSPs) are dealing not only with new technology but also the security requirements that come with it.

Facing these challenges on the frontline are enterprise and provider IT and security managers, who will be charged respectively with overseeing the deployment and maintenance of new advanced networks and the related security issues. Network security consists of the provisions and policies to prevent and monitor unauthorized access, misuse, modification or denial of a computer network and network-accessible resource. Network Security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned a password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everybody jobs conducting transactions and

communications among business, government agencies and individuals.

As the global Computer Technology undergoes a rapid evolution, it will be critical for computer and IT departments to have a strong understanding of the new Computer network architecture, security implementation, and ultimately who will be responsible for what. Once by enabling services and technologies – such as IoT, IPv6, and machine-to-machine (M2M) – become the de facto standard within the Computer s landscape, operators and their departments and security managers will need to face, understand, and overcome a whole new set of security challenges that will be more complex than anything that's come before.

Challenges for Computer Networks

a) A lack of qualified, experienced personnel to tackle security issues.

b) Lack of budget to train staff and implement security solutions.

c) Too many immediate fires to put out that security get shoved to the back of the line.

d) Lack of visibility into the overall network environment.

Since Computer and IT departments will need to overcome these issues while running a next generation computer network, they will need help from a trusted partner that understands the network layer, the customer layer, and the security layer. This help must encompass proven expertise in various data types, such as customer data, transaction data, and network data, to ensure that sensitive information is compartmentalized and safe from a variety of threats. Good skills in security architecture can buttress effective security through a number of techniques, including segmentation.

Securing Computer Networks becomes even more complex when network slicing, the ability to create multiple simultaneous mini-networks that operate under different sets of security and service requirements, enters the picture. This ability to invoke a security instance quickly for a specific period of time, in a specific place, will make security an even higher priority and that's much more of a challenge for IT and security managers, who will be the ones tasked with securing these various data types.

Security Approach

Sound security architecture including network segmentation and a full suite of interoperable security tools;

- A dedicated security organization to support continuous diagnostics and monitoring of Computer networks and data;
- Support for established security protocols and standards;
- Strong focus on personal data security and privacy, including identifying and protecting sensitive information;
- Auditing and assurance mechanisms to provide customers the best possible security infrastructure for the vendor's products, solutions, and services.

Common threats, vulnerabilities

It will be good if the networks are built and managed by understanding everything. The problem is that there are users who are

familiar and who stole the data embarrass the company and will confuse everything. It needs little effort to fight against with the threats on the computers and networks. The vulnerability will make the threat as reality. It includes wireless network security, threats and mitigation techniques which helps perform better.

Overview of Artificial Intelligence

The application Artificial Intelligence techniques have been widely appreciated in Computer Networks in particular, as well as in other fields. This inter-disciplinary endeavor has created a collaborative link between Computer Scientists and Network Engineers in the design, simulation and development of Computer Network Security models and their characteristics. Computational Intelligence (CI), an offshoot of AI, covers all branches of science and engineering that are concerned with the understanding and solving of problems for which effective computational algorithms do not yet exist. Thus, it overlaps with some areas of Artificial Intelligence and a good part of Pattern Recognition, Image Analysis and Operations Research. It is based on the assumption that thinking is nothing but symbol manipulation. Thus, it holds out the hope that computers will not merely simulate intelligence, but actually achieve it. CI relies on heuristic algorithms such as in Fuzzy Systems, Neural Networks, Support Vector Machines and Evolutionary Computation.

AI naturally transformed into Computational Intelligence (CI) with the introduction of the concept of Machine Learning. This is a scientific aspect of AI that is concerned with the design and development of algorithms that allow computers to learn based on data, such as a network intrusion log acquired over a considerable period of time. A major focus of machine learning research is to automatically learn to recognize complex attributes and to make intelligent decisions based on the correlations among the data variables. Hence, machine learning is closely related to fields such as statistics, probability theory, data mining, pattern recognition, artificial intelligence, adaptive control, and theoretical computer science.

The machine learning concept can be categorized into three common algorithms viz. supervised, unsupervised and hybrid learning. Supervised learning is the type of machine learning technique in which the algorithm generates a function that maps inputs to the desired outputs with the least possible error. Unsupervised learning is the machine learning technique in which a set of inputs are analyzed without the target output. This is also called clustering.

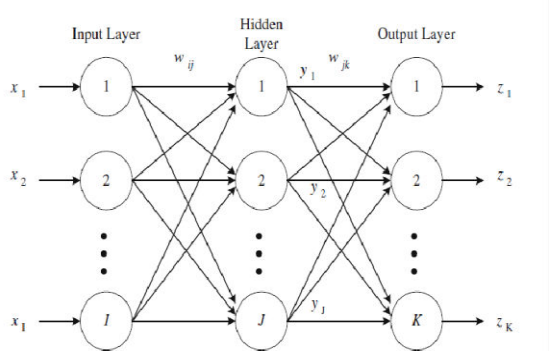
The hybrid learning combines the supervised and unsupervised techniques to generate an appropriate function and to meet a specific need of solving a problem. The computational analysis of machine learning algorithms and their performance is a branch of theoretical computer science known as computational learning theory.

OVERVIEW OF SOME ARTIFICIAL INTELLIGENCE TECHNIQUES AND THEIR APPLICATION

Artificial Neural Networks (ANN)

An artificial Neural Network consists of a collection of iterations to transform a set of inputs to a set of desired outputs, through a set of simple processing units, or nodes and connections between them. Subsets of the units in the iteration are input nodes, output nodes, and nodes between input and output form hidden layers; the connection between two units assigned some weight, used to determine how much one unit will affect the other.

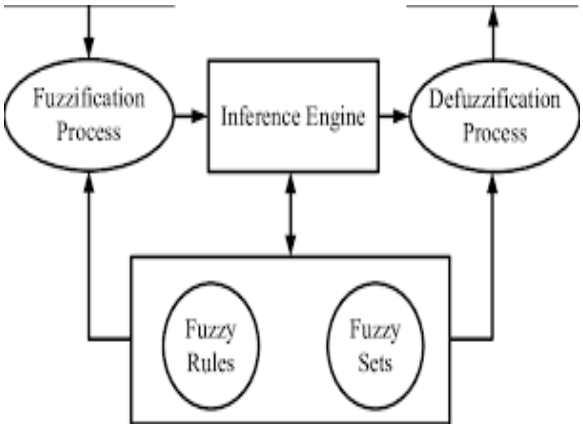
Two types of architecture of Neural Networks can be distinguished: Supervised training algorithms, the network learn the desired output for a given input or pattern in¬ the learning phase. The well known architecture is the Multi-Level Perceptron (MLP) which is employed for Pattern Recognition problems. Unsupervised training algorithms, the network learn without specifying desired output in the¬ learning phase. The Self-Organizing Maps (SOM) algorithm is used to find a topological mapping from the input space to clusters. SOM are employed for classification problems. The most important property of a Neural Network is to automatically learn the coefficients in the Neural Network according to data inputs and data outputs. The amount of research has been conducted on the application of neural networks to Detect the computer networks intrusions are very limited. Artificial neural networks offer the potential to resolve a number of the problems encountered by the other current approaches to Network intrusion detection. Artificial neural networks have been proposed as alternatives to the statistical analysis component of anomaly detection systems. Advantages of Neural network in cyber security several case studies emphasize that the use of Artificial Neural Networks (ANN) can establish g pattern recognition and identify attack in situations where rules are not known. A neural network approach can be adapted to certain constraints; to recognize patterns and compare recent actions happened with the usual behavior which allows resolving many issues even without human intervention. The technology promises not only to detect misuse and improve the recognition of malicious events with more consistency. A neural network is able to detect any possibility of misuse happened, which allows the system administrator to protect their entire organization through enhanced flexibility against intrusions. The experts believe that NN will function with more reliability and accuracy in identifying intrusions of insecure networks. The ability of the artificial neural network to identify indication of intrusion is dependent on the training requirement of data and methods which are very critical to use. The training requires thousands of individual intrusion in sequence which is very sensitive to obtain. The most significant disadvantage in applying neural network to intrusion detection system is the 'Black box' nature of neural network. The "Black Box Problem" has plagued neural networks in a number of applications. This is an on-going area of neural network research.



Fuzzy Inference Systems (FIS)

With the increase in computers getting connected to public access networks (eg: internet), it is impossible for computer systems to get protected from network intrusions. It is better to identify and remove intrusions at the initial moment rather than looking them after they enter the event. Because, there is no ideal solution to avoid intrusions from the event. One approach to handle suspicious behaviours inside a network is Artificial Intelligence. AI techniques such as neural networks and fuzzy logic are applied for detecting suspicious activities in a network, in which

fuzzy based system provides significant advantages over other AI techniques. Researchers are focussing on fuzzy rule learning for effective intrusion detection. Fuzzy logic is appropriate for the intrusion detection problem for two major reasons. First, many quantitative features are involved in intrusion detection. The second motivation for using fuzzy logic to address the intrusion detection problem is that security itself includes fuzziness. In order to evaluate all the fuzzy rules, and to take a decision, the aggregation and defuzzification is used.

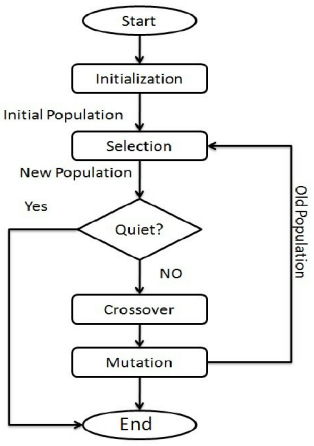


Support Vector Machines

Support Vector Machines (SVMs) are among the most popular classifi- cation techniques adopted in security applications like malware detection, intrusion detection, and spam filtering. However, if SVMs are to be incorporated in real-world security systems, they must be able to cope with attack patterns that can either mislead the learning algorithm (poisoning), evade detection (evasion), or gain information about their internal parameters (privacy breaches). The main contributions of this chapter are twofold. First, we introduce a formal general framework for the empirical evaluation of the security of machine-learning systems. Second, according to our framework, we demonstrate the feasibility of evasion, poisoning and privacy attacks against SVMs in real-world security problems. For each attack technique, we evaluate its impact and discuss whether (and how) it can be countered through an adversary-aware design of SVMs. Our experiments are easily reproducible thanks to open-source code that we have made available, together with all the employed datasets, on a public repository

Genetic Algorithms

Genetic algorithms are inspired by Darwin's theory about evolution. Solution to a problem solved by genetic algorithms is evolved. Algorithm is started with a set of solutions (represented by chromosomes) called population. Solutions from one population are taken and used to form a new population. This is motivated by a hope, that the new population will be better than the old one. Solutions which are selected to form new solutions (offspring) are selected according to their fitness - the more suitable they are the more chances they have to reproduce. This is repeated until some condition (for example number of populations or improvement of the best solution) is satisfied.



Functional Networks

Functional Networks (FN) is an extension of Artificial Neural Networks which consists of different layers of neurons connected by links. Each computing unit or neuron performs a simple calculation: a scalar, typically monotone, function *f* of a weighted sum of inputs. The function *f*, associated with the neurons, is fixed and the weights are learned from data using some well-known algorithms such as the least-squares fitting algorithm.

The main idea of FN consists of allowing the *f* functions to be learned while suppressing the weights. In addition, the *f* functions are allowed to be multi-dimensional, though they can be equivalently replaced by functions of single variables. When there are several links, say *m*, going from the last layer of neurons to a given output unit, we can write the value of this output unit in several different forms (one per different link). This leads to a system of $m-1$ functional equations, which can be directly written from the topology of the Neural Network. Solving this system leads to a great simplification of the initial functions f associated with the neurons.

CONCLUSION

Given the review of the application of Artificial Intelligence in securing computer networks and its advances along with their

Excellent performance in literature, we conclude that further research in this area is necessary as there are very promising results that are obtainable from such techniques. The ensemblage and hybridization of various Artificial Intelligence techniques also indicate a bright future in the analysis of security and the prediction of its various

Properties for effective real-time network security.

REFERENCES

1. Fatai Adesina Anifowose, Safiriyu Ibiyemi Eludiora, World Applied Programming, Vol (2), No (3), March 2012. 158-166

2. C. Sampada, S. Khusbu, D. Neha, M. Sanghamitra, A. Abraham, and S. Sugata, "Adaptive Neuro-Fuzzy Intrusion Detection Systems", in Proceedings: International Conference on Information Technology: Coding and Computing (ITCC'04), DOI: 0-7695-2108-8/04, 2004.

3. Inadyuti Dutt, Soumya Paul, " Security in All-Optical Network using Artificial Neural Network" in International Journal of Advanced Research in Computer Science, Volume 3, No. 2, March-April 2012.

4. Suleyman Kondakci, "Intelligent network security assessment with modeling and analysis of attack patterns", Security and Communication Networks, vol. 5, no. 12, pp. 1471-1486, 2012.

5. J Ryan, M-J Lin, R Miikkulainen, "Intrusion Detection with Neural Networks" in Advances in Neural Information Processing Systems 10, Cambridge, MA:MIT Press, 1998.

6.J Luo, SM Bridges, Mining Fuzzy Association Rules and Fuzzy Frequency Episodes for Intrusion Detection. International Journal of Intelligent Systems, John Wiley & Sons, vol. 15, pp. 687-703, 2000.

7. Marty, R. (2018, January 11). AI in Cybersecurity: Where We Stand & Where We Need to Go. Retrieved March 12, 2018,