Journal of Applied Mathematics & Bioinformatics, vol.5, no.3, 2015, 113-123
ISSN: 1792-6602 (print), 1792-6939 (online)
Scienpress Ltd, 2015

Implementation of Artificial Intelligence in INFOSEC tasks and applications

G. Karapilafis[1]

Abstract

Today, Information and System Security is one of the most challenging areas of research and development in modern communication. More than ever, information has immeasurable value. In data communication systems, data security is of prime concern. Similar brain performance of Artificial Neural Networks, their adaptive learning and performance of real time operations could give a significantly high potential of developing a wide range of even better Information and System security applications, including cryptographic methods, biometrics, Intrusion Detection Systems, anti-phishing and anti-malware methods etc. Merging Artificial Neural Network and INFOSEC related tasks and applications could give a great potential on security concerns.

This paper discusses the implementation of Artificial Intelligence in INFOSEC tasks and applications and the new perspective this could give.

[1] Garibaldi 26, Thessaloniki, PC:54642, E-mail: evelpil@gmail.com

Article Info: *Received* : November 12, 2014. *Revised* : February 12, 2015.
Published online : September 15, 2015.

Mathematics Subject Classification: 62M45

Keywords: Information Security; Artificial Intelligence; Artificial Neural Networks

1 Introduction

Artificial Intelligence is a term for which many descriptions have been given for. One of the most successful ones might be the following: "Artificial Intelligence is the attitude of a machine, that if it could be noticed to a human, it could justify its characterizations as intelligent" (Turban, Aronson, 1998). "The following could be considered as signs of intelligence:

-The knowledge ability or comprehension through experiences

-The export of results through contrasting or fuzzy elements

-The successful reaction in new situations

- The usage of a knowledge mechanism in troubleshooting

- The ability of thinking and exporting results

- The ability in recognition of specific elements' significance in a situation" [1].

Generally, an Intelligent Information System can demonstrate a behavior similar to human intelligence like learning, self-evaluating their results and taking decisions depending on imperfect, fuzzy or minimal data. Such, Intelligent Systems have been used by many fields as diverse as engineering, medicine, business and achieved many successes and as it seems in Information Security Industry, which deals every day with the necessity of immediate assessment of the riskiness of certain factors, usually in a fuzzy complicated environment with a limited disposal of data, which is a task that might be undertaken well by the above-mentioned intelligent systems.

2 Neural Networks and Cluster Analysis

2.1 Artificial Neural Network Function

It is not the scope of this paper to deeply explain the function of Neural Networks, but it is considered as necessary to have a look at some basic principles. Neural Networks' function is inspired from the construction and function of the human brain and its basic element, the neural, which builds a thick communication network between them. An Artificial Neural Network is a network that is initially trained and large amounts of data and rules are feed as input to it. It is the same as the brain performs a particular function. It consists of a pool of simple processing units which communicate by sending signals to each other over a large number of weighted connections.

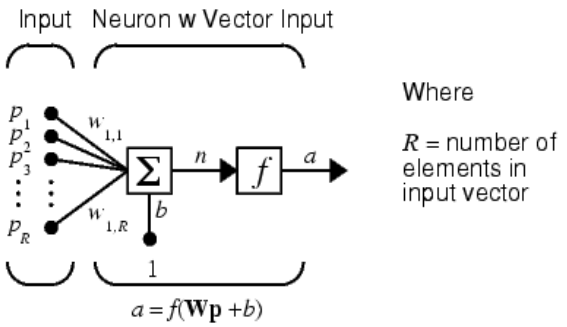

Figure1: Representation of a neural network

The network has to be trained so that the set of inputs produces the desired set of outputs. This connection list model gives the opportunity to create intelligent algorithms and procedures related with intelligence such as learning, memory, generalization and pattern batch. This model also produces computational power. Through the training process, the evaluation, the choice of the structure of the neural network, the training functions and many other factors and since we

previously know which result we want to have, we can end up having trained neural networks for specific tasks which produce logical results when we present them with new, first-seen data. Artificial Neural Networks, as humans, learn by examples. They have the ability to derive meaningful data from complex dataset and can be used to mine patterns that are too difficult for humans to be noticed. Some of their advantages may be considered the following:

- Nonlinearity: We can model classification problems where the output values are not directly related to its input
- Adaptive: Neural Networks can adjust the weights based on the changes of its surrounding environments
- Generalization: Neural Networks are able to find the suitable output for the inputs that does not exist in the training data

Researchers have already managed to build software that takes advantage of Neural Network characteristics and perform functions similar of a human brain, like voice and face recognition, autonomous navigation, decision making, logic, building a strategy and of course functions that are applicable to Information Security.

2.2 Neural Network characteristics and applicability to INFOSEC

As Information and System Security and Artificial Intelligence are two fields of science that by their definitions and their associated applications are complicated and multidimensional it is difficult to provide in a single paper all the perspectives that the combination of the above mentioned fields could give. For that reason only some basic characteristics of Artificial Neural Networks and a limited number of examples will be presented in this paper and not so analytical and specific results that researches have given so far.

One neural networks' feature that is suitable for security design is considered its learning ability. Given a specific task to solve, neural network can use a set of observations to solve this task in an optimal sense. There are two existing methods of how we can train a Neural Network. The supervised and the unsupervised learning method.

In supervised training both the inputs and the outputs are provided. The network then processes the inputs and compares its resulting outputs against the desired outputs. Errors then are propagated back through the system, causing the system to adjust the weights which control the network. There are commercial network development packages that provide tools to monitor how well an artificial neural network is converging on the ability to predict the right answer. These tools allow the training process to go on for days stopping only when the system reaches some statistically desired point, or accuracy. When finally the system has correctly been trained the weights can, if desired, be frozen. In some systems this finalized network is then turned into hardware. Other systems do not lock themselves in, but continue learning while in production use. As building a secure system and allowing its access with strong passwords is of a prime concern, the above mentioned learning method could be taken as an advantage to build another authentication mechanism for password based systems. By training an Artificial Neural Network to recognize one specific password as the right one and by limiting the errors of this process near to 0 values, a unique network with unique values is created. These specific values could be used each time as the authentication ticket. This method gives another important advantage to the user. Using different strong passwords that are changed in reasonable time periods for the different systems or networks we use, is considered as the most secure way to protect our data from disclosure but at the same time is the one that demands big effort for the user to remember. That also could me changed by using Artificial Neural Networks in the security design of our systems. That is justified by the fact that every time we train a neural network to recognize a specific password, we are

taking back different values for that very same password. This feature could facilitate users and could let them use the same password for all the networks and systems they use, by just retraining the neural network for this password.

In unsupervised training, the network is provided with inputs but not with desired outputs. The system itself must then decide what features it will use to group the data. This adaption to the environment is the promise which would enable sophisticated software to continually learn on its own as it encounters new situations and new environments. Such an environment is cyber defense where security analysts and network administrators try to discover possible security breaches to their systems. As it is said, antivirus use signature based, pattern matching mechanisms and in most of the cases if there is not an exact known signature for an attack the possibility of a compromise will be high and at the same time there will be no evidence of what hit the system. Malware developers also prove constantly by using various techniques their ability to develop malware that remain hidden during infection and operation perfectly hiding their operation from modern anti-malware software, which try to identify such a malicious software by just comparing and searching for defined signatures. This happens because criminals are constantly evolving and as it seems, this will be always a game of the cat and the mouse between evil-motivated people and legitimate users. The implementation in such examples of Artificial Intelligence techniques and software would give a great boost to Information and System Security industry. Artificial Intelligence could adapt to this environment during peace time and prepare itself to fend against unknown threats during an attack, or speed up its reaction time and precision when a known attack is taking place, leaving the administrators unbothered. Decision making under uncertain conditions, where there is lack of total knowledge and lack of time could be transformed in an easier and less stressful process for network administrators. Most of our decisions are taken under uncertainty with high risk since the evaluation is done with fuzzy and incomplete information. In such a fuzzy environment Artificial Intelligence

mechanisms could adapt very well and evaluate the risk every time it is needed so.

A more detailed example of such an implementation of Artificial Intelligence is a recent research [8] that uses Evolving Spiking Neural Networks for identifying Packed Executable and the existence of malware software, while performing classification. Code packing is a technique used to hide malicious code and perplex analysts' examination of it. One advantage of such an implementation is its low need of computational power and resources compared to already existing software where there is the need to always unpack the code if there is not signature verified. Usage of evolving Spiking Neural Networks reported promising results indicating the importance and the dynamics that the implementation of Artificial Intelligence in Information Security and Assurance could have.

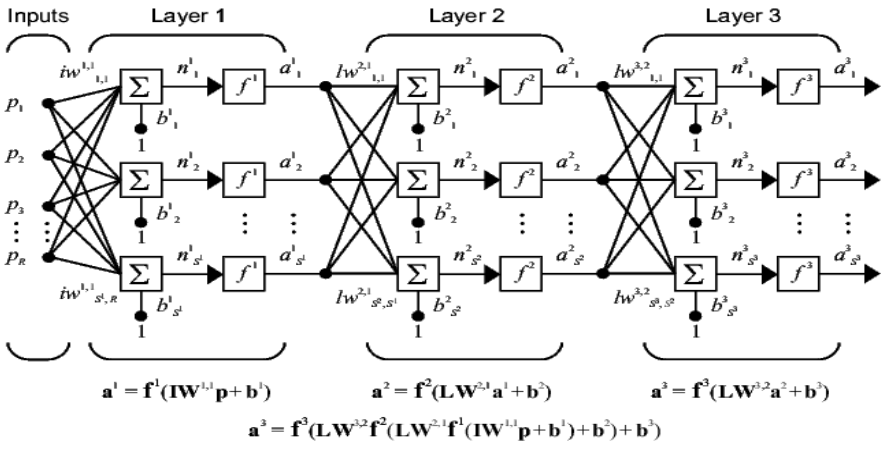

Figure 2: Neural Network that consists of three levels and neurons to each level

A second feature is the one-way property that has to do with the computation of the output from the input. In Neural Networks it is easy to compute the output from the input, while difficult or impossible to compute the input from the output. This can be seen in the following function (1) of a simple neuron model.

$$C = f\left(\sum_{i=0}^{n-1} w_j p_j + b\right) \quad (1)$$

It is easy to compute C from P, while difficult to compute P from C. This property is often required by Hash function used for data integrity and generally in asymmetric algorithms, which crux is that they provide security by using mathematical equations that are easy to perform in one direction and next to impossible to perform in the other direction. With such a characteristic of neural networks, a password identity based security system could get a new direction of development and also data integrity mechanisms.

2.3 Cluster Analysis

Last years there has been an effort from researches to find a meaning and a structure inside chaotic systems. With classical statistics the effort of finding an interconnection between the data of those systems is considered as tricky.

Cluster analysis is a term that firstly was used in 1939 from Tryon and refers to the effort of finding specific structures inside a dataset, with the usage of some different algorithms that aim to the classification of the data. In the following picture is presented an example of cluster analysis.

The intension is the identification of the clusters with definite visual separation and moreover the specification of the degree of participation of the data to one cluster. This specification is one of the main differences between cluster analysis (fuzzy statistics) and classical statistics. Classical statistics most of the time cannot designate a specific value to a certain category. On the other hand with cluster analysis a degree of participation is assigned to all data. Cluster analysis is very useful in pattern analysis, decision making, data mining etc.

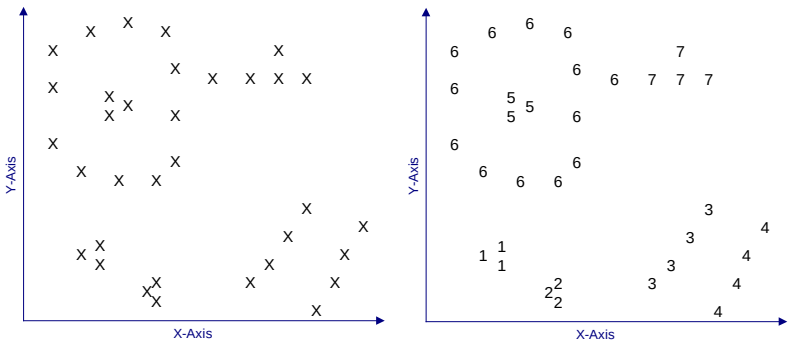

Figure 3: An example of Cluster Analysis

Fuzzy C-Means Clustering is an algorithm that is used in cluster analysis. It was firstly introduced from Bezdek. In general, we could say that fuzzy clustering extends the meaning that “one data belongs to a cluster” and relates every data with every cluster by assigning them a degree of participation to the clusters.

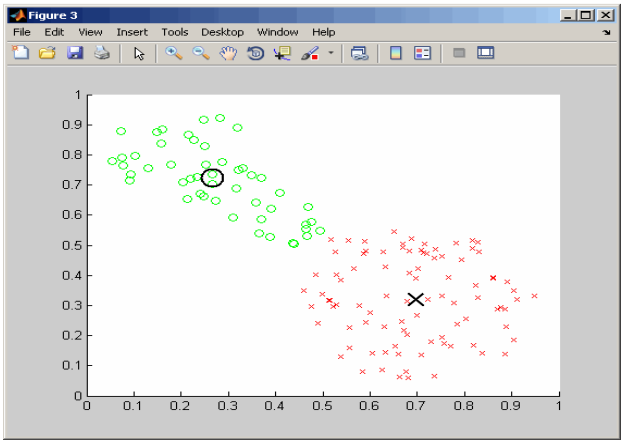

Figure 4: Determination of the center of the clusters

In such a way, we could take the advantages that cluster analysis gives us and try to classify web sites for example and see how many clusters we can get and in which of them the websites we are interested in participate more or less. Phishing or legitimate websites could be evaluated and classified using that way, giving a new approach of doing this.

4 Discussion and Conclusions

The rapid development of computer systems and the increase of sophistication in computer security attacks, make Artificial Intelligence a valuable field in assuring computer security for the future. Whether Artificial Intelligence will be used as an assistant or be used as the full time security administrator, it is highly probable that it will be utilized in computer security since the computer systems' world is turning to more adaptive and automated systems. The design of intelligent information systems is considered as necessary not only in the field of information security but also in our every day lives. Artificial Intelligence is a part of science that has applicability in many fields. Discovering its capabilities is an undergoing process but it has already proven that new horizons are opened as long as the human race advances in its understanding of mathematics and as processing power increases.

References

[1] L. Iliadis, *Artificial Intelligence Systems and applications in danger estimation*, 2007.

[2] M.T. Hagan and H.B. Beale, *Neural Networks Design*, Boston, MA, PWS Publishing, 1996.

[3] S. Haykin, Multilayer Perceptron in *Neural Networks and Learning Machines* 3rd Ed., Publishing as Pearson Prentice Hall, ch.4.pp.122-139, 2009.

[4] http://www.mathworks.com/help/toolbox/bioinfo

[5] L. Iliadis, M. Vangeloudh and S. Spartalis, An intelligent system employing an enhanced fuzzy *c*-means clustering model: Application in the case of forest fires, *Computers and Electronics in Agriculture*, **70**(2), (2010), 276-284.

[6] V. Kecman, *Learning and Soft Computing* MIT, Press, USA, 2001.

[7] V. Vapnik, *Statistical Learning Theory, The support vector method of function estimation*, 1998.

[8] K. Demertzis and L. Iliadis, *Evolving Computational Intelligence System for Malware Detection*, 2014.