Middle-East Journal of Scientific Research 24 (10): 3329-3331, 2016
ISSN 1990-9233
© IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.3329.3331

Unsupervised Feature Learning and Deep Learning in Artificial Intelligence for Enhancing Cyber Security

S. Kanthraj and B.E. Student

Department of Computer Science & Engineering, the National Institute of Engineering, Mysore, India

Abstract: Security in the cyber field is the most important factor to protect the data either in public or private sector. Many supervised algorithms are created just to protect the data from the intruder or hacker. But during the time of attack it is not sure that these algorithms are sufficient enough to solve those attacks. Only timing and efficiency matters in this field. Deep learning in Artificial Intelligence comes into picture when we talk about the efficiency, automation, delay timing etc. Unsupervised feature learning is a method in deep learning to recognize meaningful raw data from an unstructured data. In this paper enhancing cyber security by means of unsupervised feature leaning and deep learning in Artificial Intelligence is discussed.

Key words: Security risks · Deep learning · Featured learning

INTRODUCTION

Deep learning, while sounding flashy, is really just a term to describe certain types of neural networks and related algorithms that consume often very raw input data [1]. They process this data through many layers of nonlinear transformations of the input data in order to calculate a target output.

Unsupervised feature extraction is also an area where deep learning excels. Feature extraction is when an algorithm is able to automatically derive or construct meaningful features of the data to be used for further learning, generalization and understanding. More generally, deep learning falls under the group of techniques known as feature learning or representation learning. Paraphrasing Wikipedia, feature learning algorithms allow a machine to both learn for a specific task using a well-suited set of features and also learn the features themselves. In other words, these algorithms learn how to learn.

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards [2]. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. A range of traditional crimes are now being perpetrated through cyberspace. This includes the production and distribution of child pornography and child exploitation conspiracies, banking and financial fraud, intellectual property violations and other crimes, all of which have substantial human and economic consequences.

Cybersecurity Risks: The main cause of cyber-attack is secured software system error instead of other causes such as hardware failures. Many organizations have studied cyber-attacks and have discovered repeated occurrences of task management errors in which the soft process chose to utilize the wrong thread [3]. These errors in the layers of processing can cause firewall and other security software malfunctions and have disastrous consequences for highly protected environments such as nuclear power plant. The primary concern is to have high security while minimizing the delay [4]. The risks associated with any attack depend on three factors: threats (who is attacking), Vulnerabilities (the weaknesses they are attacking) and impacts (what the attack does). The management of risk to information systems is considered fundamental to effective cybersecurity.

Deep Learning and Unsupervised Learning: Machine learning is a very successful technology but applying it today often requires spending substantial effort hand-designing features. This is true for applications in vision, audio and text. Deep Learning algorithms are

Corresponding Author: S. Kanthraj, Department of Computer Science & Engineering, the National Institute of Engineering, Mysore, India.

based on building massive artificial neural networks that were loosely inspired by cortical (brain) computations [1]. Deep learning has been used successfully in many applications and is considered to be one of the most cutting-edge machine learning and AI techniques at the current time. The associated algorithms are often used for supervised, unsupervised and semi-supervised learning problems [5]. Learning is improving a knowledge system by extending or rearranging its knowledge base or by improving the inference engine. This is one of the most interesting problems of artificial intelligence that is under intensive investigation. Machine learning comprises computational methods for acquiring new knowledge, new skills and new ways to organize existing knowledge. Problems of learning vary greatly by their complexity from simple parametric learning which means learning values of some parameters, to complicated forms of symbolic learning [5]. AI provides methods for both -- supervised learning (learning with a teacher) as well as unsupervised learning. The latter is especially useful in the case of presence of large amount of data and this is common in cyber defence where large logs can be collected. Data mining has originally grown out of unsupervised learning in AI. Unsupervised learning can be a functionality of neural nets, in particular, of self-organizing maps. A distinguished class of learning methods is constituted by parallel learning algorithms that are suitable for execution on parallel hardware. These learning methods are represented by genetic algorithms and neural nets.

How Is this Achieved?

This can be done by,

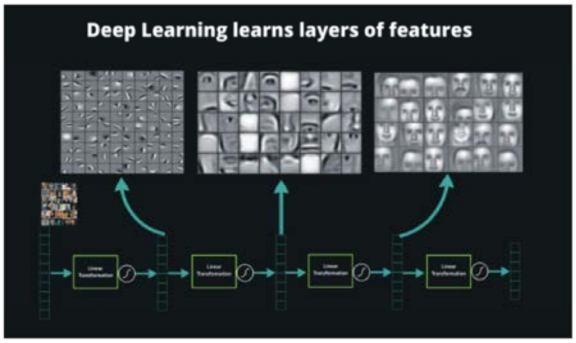
Artificial Neural Network (ANN): ANN is a mathematical model that consists of an interconnected group of artificial neurons which processes the information [3]. ANN are used to model complex relationships between inputs and outputs or to find patterns in data. In this a neuron calculates the sum by multiplying input by weight and applies a threshold. The result is transmitted to subsequent neurons. Basically, the ANN has been generalized to [6]:

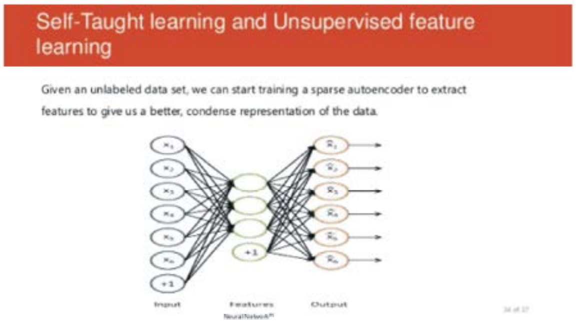
$$yi = f(\sum_{k} wikxk + \mu i)$$

where wik are weights attached to the inputs, xk are inputs to the neuron i, ìi is a threshold, f (•) is a transfer function and yi is the output of the neuron.

Fuzzy Inference Systems (FIS): Sampada *et al*. [7] proposed two machine learning paradigms: Artificial Neural Networks and Fuzzy Inference System, for the design of an Intrusion Detection System nothing but Cyber Security. They used SNORT to perform real time traffic analysis and packet logging on IP network during the training phase of the system. They constructed a signature pattern database using Protocol Analysis and Neuro-Fuzzy learning method. They then tested and validated the models using the 1998 DARPA Intrusion Detection Evaluation Data and TCP dump raw data [3]. Their experiment also showed the importance of variable selection, as the two techniques performed worse when all the variables were used without selection of the variables.

Images Represents Feature Learning:


Deep Learning learns layers of features


Self-Taught learning and Unsupervised feature learning

Given an unlabeled data set, we can start training a sparse autoencoder to extract features to give us a better, condense representation of the data.

CONCLUSION

The field of artificial intelligence gives the ability to the machines to think analytically, using concepts. Tremendous contribution to the various areas has been made by the Artificial Intelligence techniques such as deep learning from the last decade. Artificial Intelligence will continue to play an increasingly important role in the various fields. This paper is based on the concept of enhancing cyber security by using deep learning techniques for efficient error detection and proper timing when an attack occurs. I conclude that further research in this area can be done as there are very promising and profitable results that are obtainable from such techniques. While scientists have not yet realized the full potential and ability of artificial intelligence, this technology will likely have far-reaching effects on human life in the years to come.

REFERENCES

1. http://www.innoarchitech.com/artificial-intelligence-deep-learning-neural-networks-explained.
2. https://www.dhs.gov/cybersecurity-overview
3. Artificial Intelligence and its Application in Different Areas, Avneet Pannu, International Journal of Engineering and Innovative Technology (IJEIT), 4(10), April 2015.
4. Cybersecurity Issues and Challenges: In Brief, Eric A. Fischer Senior Specialist in Science and Technology, August 12, 2016.
5. Artificial Intelligence in Cyber Defense, Enn Tyugu, 2011. 3rd International Conference on Cyber Conflict.
6. Fatai Adesina Anifowose, Safiriyu Ibiyemi Eludiora, 2012. “Application of Artificial Intelligence in Network Intrusion Detection”, World Applied Programming, 2(3).
7. Deepa, S.N. and B. Aruna Devi, 2011. “A survey on artificial intelligence approaches for medical image classification”, Indian Journal of Science and Technology, 4(11).