|  |  |
| --- | --- |
| **Title** | Training Artificial Neural Network using Particle Swarm Optimization Algorithm |
| **Authors** | * Roy, Argha * Dutta, Diptam * Choudhury, Kaustav |
| **Publication** | International Journal of Advanced Research in Computer Science and Software Engineering |
| **Date Published** | March 2013 |

Roy, A., Dutta, D., & Choudhury, K. (2013). Training Artificial Neural Network using Particle Swarm Optimization Algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering*, *3*(3), 430–434. https://doi.org/10.1109/icecco.2013.6718256

**Abstract**

In this paper, the adaptation of network weights using Particle Swarm Optimization (PSO) was proposed as a mechanism to improve the performance of Artificial Neural Network (ANN) in classification of IRIS dataset. Classification is a machine learning technique used to predict group membership for data instances. To simplify the problem of classification neural networks are being introduced. This paper focuses on IRIS plant classification using Neural Network. The problem concerns the identification of IRIS plant species on the basis of plant attribute measurements. Classification of IRIS data set would be discovering patterns from examining petal and sepal size of the IRIS plant and how the prediction was made from analyzing the pattern to form the class of IRIS plant. By using this pattern and classification, in future upcoming years the unknown data can be predicted more precisely. Artificial neural networks have been successfully applied to problems in pattern classification, function approximations, optimization, and associative memories. In this work, Multilayer feed-forward networks are trained using back propagation learning algorithm.

**Reason**

This research is quite complex but from what I understand, the topic is at the very heart of deep learning algorithms which are involved in machine learning. If given the chance, I would like to learn more about this field as it is quite interesting and challenging. Applying such algorithms to neural networks which imitate how neurons signal one another, which is currently out of my capabilities and knowledge.

|  |  |
| --- | --- |
| **Title** | Proposed efficient algorithm to filter spam using machine learning techniques |
| **Authors** | * Aski, Ali Shafigh * Sourati, Navid Khalilzadeh |
| **Publication** | Pacific Science Review A: Natural Science and Engineering |
| **Date Published** | November 2016 |

Aski, A. S., &amp; Sourati, N. K. (2016). Proposed efficient algorithm to filter spam using machine learning techniques. Pacific Science Review A: Natural Science and Engineering, 18(2), 145–149. https://doi.org/10.1016/j.psra.2016.09.017

**Abstract**

Electronic spam is the most troublesome Internet phenomenon challenging large global companies, including AOL, Google, Yahoo and Microsoft. Spam causes various problems that may, in turn, cause economic losses. Spam causes traffic problems and bottlenecks that limit memory space, computing power and speed. Spam causes users to spend time removing it. Various methods have been developed to filter spam, including black list/white list, Bayesian classification algorithms, keyword matching, header information processing, investigation of spam-sending factors and investigation of received mails. This study describes three machine-learning algorithms to filter spam from valid emails with low error rates and high efficiency using a multilayer perceptron model. Several widely used techniques include C4.5 decision tree classifier, multilayer perceptron and Naïve Bayes classifier, all of which are used for training data whether in the form of spam or valid emails. Finally, the results are discussed, and outputs of considered techniques are examined in relation to the proposed model.

**Reason**

I chose this research because it is quite interesting how the researchers are able to come up with an algorithm that has higher efficiency compared to naïve Bayes classifier algorithms. Machine Learning is quite interesting to me and receiving spam emails is quite troublesome and maybe some time in the future, I would like to experiment and create my own spam filter to detect valid emails from spam.

|  |  |
| --- | --- |
| **Title** | Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review |
| **Authors** | * Dixit, Priyanka * Silakari, Sanjay |
| **Publication** | Computer Science Review |
| **Date Published** | November 2020 |

Dixit, P., &amp; Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and Status Review. Computer Science Review, 39. https://doi.org/10.1016/j.cosrev.2020.100317

**Abstract**

Cybersecurity mainly prevents the hardware, software, and data present in the system that has an active internet connection from external attacks. Organizations mainly deploy cybersecurity for their databases and systems to prevent it from unauthorized access. Different forms of attacks like phishing, spear-phishing, a drive-by attack, a password attack, denial of service, etc. are responsible for these security problems. In this survey, we analyzed and reviewed the usage of deep learning algorithms for Cybersecurity applications. Deep learning which is also known as Deep Neural Networks includes machine learning techniques that enable the network to learn from unsupervised data and solve complex problems. Here, 80 papers from 2014 to 2019 have been used and successfully analyzed. Deep learning approaches such as Convolutional Neural Network (CNN), Auto Encoder (AE), Deep Belief Network (DBN), Recurrent Neural Network (RNN), Generative Adversal Network (GAN) and Deep Reinforcement Learning (DIL) are used to categorize the papers referred. Each specific technique is effectively discussed with its algorithms, platforms, dataset, and potential benefits. The paper related to deep learning with cybersecurity is mainly published in the year 2018 in a large number and 18% of published articles originate from the UK. In addition, the papers are selected from a variety of journals, and 30% of papers used are from the Elsevier journal. From the experimental analysis, it is clear that the deep learning model improved the accuracy, scalability, reliability, and performance of the cybersecurity applications when applied in real-time.

**Reason**

This research is a compilation of algorithmic approaches that involve user safety on the Internet. I also find this field interesting as cybersecurity is ever evolving and it would be good to learn such approaches and how these would be beneficial against certain cyber-attacks. As deep learning algorithms have improved the performance of cybersecurity applications, there is still room for tweaks or even a completely new algorithm to be found to improve efficiency and accuracy in detecting potential external attacks.