***Deep Learning-Based Intrusion Detection***

Deep learning is a new paradigm In the field of machine learning primarily built with Artificial neural networks or artificial neural networks and have a higher percentage of A form of other traditional machine learning techniques Deep learning consists of different networks such as:

Convolutional Neural Networks (CNNs), Deep Belief Net-works (DBNs), Restricted Boltzmann Machines (RBMs), and Recurrent Neural Networks (RNNs), each of which has different capabilities and properties.

This article is on deep learning-Certified Intrusion Detection Comprehensive Scan of different nuts from 2010 to 2020. However, it will be more useful before the advent of the survey, first displays the key terms and know the background schemes of IDS and make a brief Describes the techniques of the previous character. Steps of the intrusion detection process, such as Selection/extraction and classification.

According to our studies, this is the first paper that aims to explore intrusion detection systems that use deep learning networks. The contribution of this survey article can be listed:

• Intrusion Detection Scan, • Intrusion Detection Review, • Intrusion Detection Overview, • Anomaly detection scanning, • Anomaly detection review, • Anomaly detection overview, • Scan to detect abuse• Misuse detection audit, • Usage discovery discovery overview.

Module: CNN is another step for classification. The author showed that their model achieves fewer false alarms high rate Accurate compared to other CNN-based IDS systems.

Submit a NIDS form that uses CNNs, where CNNs are automatically combined determine the initial network traffic. Data processing With CNN, this scheme diverts raw network traffic Vector to 2D image format.

Module: IDS schemes is Snort, which is a free and open-source IDS tool that can be used on small networks. It can be run on operating systems such as BSD, Linux, Windows, and Mac.Furthermore, Snort doesn’t need to recompile the kernel anddoes not need specific hardware or software. In additionto the before-mentioned environments, recently other soft-ware tools such as DeepLearning4j, Caffe, Torch,Theano,MXNet, Neon, and Microsoft Cognitive Toolkit can be used for designing deep learning-based solutions.

Results achieved on the UNSW-NB15 dataset by some IDS solutions based on deep learning. As shown in this numbers, fewer charts evaluated newer data sets, and In future studies, the proposed schemes should be verified They are evaluated on newer data sets that better reflect reality Traffic in the target environment Its deep learning methods They were used for classification and learning purposes,the latter method reduces the complexity of the rawDataset features. As described in the previous sections, auto-Encoders are often used to learn features, while RNNs are used Provided for Classification Purposes. Regarding the need to IDS systems in real time, online learning method is applied In some deeply studied IDS approaches. Also, online Learning cannot be easily parallelized, and all input data It has a similar distribution and possession Specific amount of link. In this learning method, data Distributions varying over time can be a challenging problem.Accordingly, dealing with such challenges in the Internet Learn and apply the suggested methods in depth IDS schemes should be investigated.

This article provides an in-depth review and rating of intrusion detection schemes that benefited deep neural networks to deal with intrusions and maliciousness behaviors. For this purpose, it first ranks deep IDS Schemes according to their built-in deep learning technology-niques and describes how each scheme tries to apply deep

Learning methods to identify the different types of intervention.Besides, in the studied deep IDS schemas, the shallow learning-Gee methods used in conjunction with deep learning Techniques are investigated. Moreover, to provide in-depth Insights into the studied IDS frameworks, in each category of The studied curricula, its basic contributions, progress-Marks and restrictions are specified. Besides, in each category, The evaluation scales used, simulations, and datasets are comparison. Finally, it can be concluded that deep learning is An interesting method, which presents many opportunities As well as challenges in the context of intrusion detection.