Deep Learning: The Many Approaches of Intrusion Detection System Can Be Implemented and Improved Upon

Trinity Taylor

Norfolk State University

Deep Learning: The many approaches of Intrusion Detection System can be implemented and improved upon

Trinity Taylor

Norfolk State University

April 15, 2022

Introduction

For my research topic I decided to look at Deep learning.Deep learning can be used in many ways for example in web searching. Deep learning can also can improve new businesses and products. Deep learning could lead to amazing discoveries. Deep learning is making a neural network learn something. In my research I talk about Intrusion detection system, traditional approach for intrusion detection, existing intrusion detection, machine learning and deep learning based intrusion detection system, and future work.

Intrusion detection system

Intrusion detection system or IDS is a second line of defense for a system. Some ways that IDS is used are access control, authentication mechanisms and encryption. These methods are used to secure the system from cyber attacks[2]. IDS can tell the difference between normal and harmful actions. This paper states that “data mining which is used to describe knowledge discovery can help to implement and deploy IDSs”[1]. If the Intrusion detection system has a higher accuracy and robust behavior than the IDS might not be as effective as the traditional approach for intrusion detection.

Traditional Approach for intrusion detection

The traditional approach for intrusion is using machine learning to make an example of trustworthy activity and all the the newly created activity is based on that precencent. The traditional method for intrusion detection also searches for known ways of cyber attacks.The studies shown in this paper were four types of machine learning discussed. The first was Naive Bayes, Artificial neural network, Support Vector Machine, an Random forest. The traditional method tends to be less effective compared to the more modern methods that will be discussed in this research paper.

Existing Intrusion detection systems (Commercial or gov organizations)

Existing Intrusion detection systems are implemented for example in the United States Department of Homeland Security. In the Department of Homeland Security they use IDS as a way to monitor computer systems and networks for unauthorized access and abuse of existing privileges[3]. Another example would be Security Event Manager or (SEM). SEM is used to alert the user about suspicious activity all day and then alert the user in real time to prevent lasting harm.[4]

Machine learning and deep learning based intrusion detection system

This next part is about machine learning and deep learning based intrusion detection systems. Machine learning can be broken up into four approaches. NaiveBayes or (NB), Artificial neural network or (ANN), Support Vector Machine or (SVM), and Random forest or (RF). NaiveBayes are used to predict the possibility of classes based on multiple attributes. Artificial neural networks are multiple processing elements that get inputs and give outputs based on a predefined activation function. SVM are used to classify, regress, and outlier detection. RF is used for sampling a random vector from a tree of predictions. The deep learning approaches that I will be discussing are split from the deep discriminative model consisting of the recurrent neural networks or (RNN), deep neural networks or (DNN), and convolutional neural networks or (CNN). The later split of models called the generative/unsupervised models. The generative/ unsupervised model will be made up of the deep autoencoders approach, the restricted Boltzmann approach, the deep Boltzmann machines approach, and the deep belief network approach.

Future work: Improve the IDS system further

Improvement can be made on IDS specifically neural networks by having at least a two layered system to supported by a layer of long short-term memory. To improve traffic detection it's recommended to use a Support Vector Machine. Using an auto encoder with non- symmetrical hidden layers improvement can classification results. To improve cyber security intrusion it is recommended to use conditional variational autoencoder and deep neural network.[1]

Conclusion

In conclusion, my experience with researching Deep learning has improved my under standing of this topic. I believe that I have improved my ability to differentiate between the many ways that you can approach deep learning. I think that I have a better understanding of machine learning as well as neural networks and how they can be implemented. This project has taught me what to expect if I were to go into graduate school so I can better prepare my self.

References:

1. Mohamed Amine Ferrag, Leandros Maglaras, Sotiris Moschoyiannis et. all, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study, Journal of Information Security and Applications", Volume 50, 2020, 102419, ISSN 2214-2126, https://doi.org/10.1016/j.jisa.2019.102419.

2. DeepLearningAI. Neural Networks and Deep Learning (Course 1 of the Deep Learning Specialization). (Mar. 2, 2020). Accessed: Apr. 13, 2022. [Online Video]. Available: https://www.youtube.com/playlist?list=PLkDaE6sCZn6Ec-XTbcX1uRg2_u4xOEky0

3. Homeland Security et. all, "Intrusion Detection and Prevention Systems", 2013, https://www.dhs.gov/sites/default/files/publications/IDPS-HLT_0813-508.pdf

4. SolarWinds, “Security event manager - view event logs remotely,” SolarWinds. [Online]. Available: https://www.solarwinds.com/security-event-manager. [Accessed: 15-Apr-2022].