Chapter 3
Review on Machine and Deep Learning Applications for Cyber Security

Thangavel M.
Thiagarajar College of Engineering, India

Abiramie Shree T. G. R.
Thiagarajar College of Engineering, India

Priyadharshini P.
Thiagarajar College of Engineering, India

Saranya T.
Thiagarajar College of Engineering, India

ABSTRACT

In today's world, everyone is generating a large amount of data on their own. With this amount of data generation, there is a change of security compromise of our data. This leads us to extend the security needs beyond the traditional approach which emerges the field of cyber security. Cyber security's core functionality is to protect all types of information, which includes hardware and software from cyber threats. The number of threats and attacks is increasing each year with a high difference between them. Machine learning and deep learning applications can be done to this attack, reducing the complexity to solve the problem and helping us to recover very easily. The algorithms used by both approaches are support vector machine (SVM), Bayesian algorithm, deep belief network (DBN), and deep random neural network (Deep RNN). These techniques provide better results than that of the traditional approach. The companies which use this approach in the real time scenarios are also covered in this chapter.

DOI: 10.4018/978-1-5225-9611-0.ch003

INTRODUCTION

In today's world, information is one of the most important aspects in almost every part of our life; the information is valuable for individual, organization, and country. Privacy is needed for such valuable information. Due to invention and innovation, is widespread use of device and technology, which makes people communication and industrial productions more sophisticated. This technology is not only providing sophistication to the information holders and users but also to the attackers. This same technology also ensures the attacker in many ways to launch attacks in a more creative way. Cybersecurity/information system security is the technique consists of protecting the systems, computer programs, data, and networks form attackers or unauthorized user, which are aimed for exploitation. The cybersecurity reduces the risk of cyber attacks; the cyber attacks are usually concentrating on accessing, destroying, changing the most sensitive information in order to create a risk to individual or organization. The Deep Learning and Machine Learning concept to break these constraints. The birth of Machine learning is started in conjunction with other technologies like virtual machines, test simulators, etc. This ML algorithm quickly scales the analysis process of information collected by the Sec Intel. The basic principle of the ML algorithm is it will improve its response by learning and learning. Nearly it will take 2-3 days for the security group to analyze the information provided by the Sec Intel, but the ML will take 1day at first learning, then reduce it slowly by learning and the next day it will take 12hours, and the next time it will take 8hours and so on., The effective scale analysis by ML is more times greater than the security group especially for the automated task so this is what the wonder of ML. But, Machine Learning can perform efficiently in small scale data and lower configured systems. This emerges the Deep Learning which is a subfield of the Machine learning approach. Deep Learning can perform well only in a tremendous amount of data and high configured systems. The main advantage of Deep Learning on cybersecurity is the deep neutral network process. This process deeply examines the data and for this study, the deep learning algorithm requires a vast amount of data. As we already know today's world generating googol of data than what about the future! yes, obviously it will become too large. For handling cyber security for this much amount of data the deep learning is the precise answer. Deep Learning algorithm is categorized into supervised deep learning and unsupervised deep learning. Supervised deep learning approach will predict only the targeted values from a set of data but in unsupervised approach, there are no such target values and it simply predicts all the possible values from the dataset. The usage of these two categories depends on the implementation of cybersecurity needs. The approach of deep learning to the field of cybersecurity ranges from the intrusion detection system for sensor networks and transport layer, Malicious Code Detection, Hybrid malware classification, Behaviour detection of Botnet, traffic identification and anomaly detection. Although, the application of deep learning for cybersecurity isn't easy. A report last week stated that a recent attack happened in a private organization. It was hacked during the midterms and that attack compromised access to their email accounts of their company, where they had been watched and spied by the hackers over a long time which included the details of their client. Even for an organization like this took a long time and a large amount of money to detect the intrusion and recover from the attack. A yet another report stated by Forbes, a major cyber-attack was traced in tax software which impacted people who belong to 64 countries. The attackers made an offer of 300 dollars of bitcoin for the retrieval of their hacked data as an initial payment. It gave lots of uneasiness to the government of the country as well as the individual victims who and all affected by this massive attack. So, these real-time attacks which clearly proves that the effort which we put on the safeness of our system will easily make us pay a lot of amount and time when it gets compromised.