Chapter 8
Using Deep Learning and Big Data Analytics for Managing Cyber-Attacks

Sarabjeet Kaur Kochhar
https://orcid.org/0000-0001-9406-7414
Indraprastha College for Women, University of Delhi, Delhi, India

Anishka Bhatia
Indraprastha College for Women, University of Delhi, Delhi, India

Nandini Tomer
Indraprastha College for Women, University of Delhi, Delhi, India

ABSTRACT

This chapter acquaints the reader to the terms and terminologies of cyber-attacks, cybersecurity, big data, data analytics, and related new age technologies, including deep learning. The types of cyber-attacks, how they become special and different within the big data analytic frameworks, a multi-layer framework for their detection, and the challenges therein are detailed next. Thereafter, an extensive review of some research works has been undertaken to provide an in-depth insight to the various cyber security detection systems using the new age technologies such as naive Bayesian networks in intrusion detection systems, deep learning in Android malware detection, and intelligent malware detection, etc. Conclusions have been drawn from these studies to establish that the emerging technologies, like artificial intelligence, machine learning, deep learning, and internet of Things, are the need of the hour to assist organizations in navigating the increasingly aggressive cyber threat landscape.

DOI: 10.4018/978-1-6684-5722-1.ch008

INTRODUCTION

Cyber-attacks are malicious efforts to steal, breach, alter, disable, or destroy web-based systems, through unauthorized access. According to an article published in Security Magazine a study was conducted by Michel Cukier, Clark Professor of Mechanical Engineering which stated that more than 2,200 cyber-attacks happen per day which equates to about one cyber-attack every 39 seconds (Clark Study School, n.d.). Cyber-attacks are rising with each passing day and therefore the severity of vandalism made by the cyber-attackers is increasing multi-fold. According to Trustwave's 2015 Global Security Report, approximately 98% of tested web applications were found vulnerable to cyber-attack (Trustwave, n.d.). Militia, Science and Research, top government agencies, businesses, healthcare, and even political groups are only some of the top targets for ransom or hacking secured information. Based on the Department of Business, Innovation and Skills' 2015 security survey 90% of the sizable organisations and 74% of the small organisations are affected by security breaches (PWC, n.d.).

Cybersecurity is at a tipping point, with the vast number of cyber-attacks, breaches, and threats increasing the need to respond quickly and precisely, before it's too late. The threat landscape is always evolving; for example, the rapid expansion of malware, ransomware (Richardson & North, 2017), DDoS (Garber, 2000), and social engineering (*Ns*, n.d.) assaults has already posed numerous issues to businesses. As an instance, a standard defence was good enough to protect any organisation from intrusions just a few years ago. Typical malware was easy to identify and targeted thousands of victims. Security solutions focused on blacklisting known malware signatures and were able to guard against the majority of attacks. However, the cybersecurity landscape — as well as modern attackers — have substantially evolved. They're clever and well-organized (many cybercrime operations are conducted like businesses), and they target specific individuals and businesses in search of lucrative targets. These hackers are quiet and sneaky, yet the damage they cause can be quite costly. Therefore, modern solutions and intelligent systems are required to deal with these cybercrimes.

In this challenging scenario, it has become need of the hour to apply Big Data Analytics and technologies like Artificial Intelligence, Machine Learning, Deep Learning and Internet of Things etc., to assist the organizations in navigating the increasingly aggressive cyber threat landscape. Big Data Analytics typically uses the Big Data to inspect, observe, and spot irregularities in the networks by analysing large amounts of data. The security-related information retrieved from Big Data has been successfully employed to cut down on the time it takes to identify and resolve a security problem. According to MeriTalk's recent U.S. government poll, 81 percent of Feds said their agency uses Big Data Analytics for cybersecurity

Related Content