Chapter 7
Cyber Threats Detection and Mitigation Using Machine Learning

Vaishnavi Ambalavanan
Pondicherry University, India

Shanthi Bala P.
Pondicherry University, India

ABSTRACT

Cyberspace plays a dominant role in the world of electronic communication. It is a virtual space where the interconnecting network has an independent technology infrastructure. The internet is the baseline for the cyberspace which can be openly accessible. Cyber-security is a set of techniques used to protect network integrity and data from vulnerability. The protection mechanism involves the identification of threats and taking precaution by predicting the vulnerabilities in the environment. The main cause of security violation will be threats, that are caused by the intruder who attacks the network or any electronic devices with the intention to cause damage in the communication network. These threats must be taken into consideration for the mitigation process to improve the system efficiency and performance. Machine learning helps to increase the accuracy level in the detection of threats and their mitigation process in an efficient way. This chapter describes the way in which threats can be detected and mitigated in cyberspace with certain strategies using machine learning.

INTRODUCTION

Cyberspace plays a major role in the today modern world. It is a place where the technologies are integrated to create an interactive illusion irrespective of the geographical location and time. This virtual environment has become a semi-conscious entity in our lifestyle like net banking, video conferencing, e-shopping, etc. The usage of electronic devices has reached millions of mobile units in both public and private sectors for a different purpose. This gradual growth is possible through technologies like Internet of things (IoT), Cloud Computing, Big Data, and Artificial Intelligence. Another important part is

DOI: 10.4018/978-1-5225-9611-0.ch007

the information storage, where the data is stored either in client or server side based on the application and the system has to maintain integrity. It can be achieved through some of the standardized security mechanisms in order to protect the resources from cyber threats like malware, ransomware, phishing, exploit-kit and application attack (Colorossi, 2015). The threats are elevated due to the technology enrichment, which creates a path to the sophisticated attackers at lower cost and thus makes the security more challenging one.

Cybersecurity deals with issues like the way in which the information is handled and delivered to the end users by holding the principle of Confidentiality, Integrity, and Availability(CIA). These destructive acts of accessing the information with malicious intention lead to cyber threats. The threats initially start with the system vulnerability, which increases the attacking rate by loopholes and back doors that are available in it. The security mechanism involves a protection scheme for the user information and the network environment in which the hacker observes the vulnerability of the systems and may attack the victim. Generally, the user information contains both personal and professional details that are more sensitive. The fact of being exposed to risk is more which are directly proportional to the confidentiality of the data. The possibility of attacks is started when the data is transferring through the public network. The network helps to route the data from source to destination. So, the intruder analyzes the network set-up to identify the possibilities of penetrations method with least time and effort to gain a higher success rate. This penetration process is often carried out by means of the weak authentication system that are maintained by the administrator. As a result, the developer can provide safeguard measures for the existing threats. But it is not easy in case of emerging threats on a daily basis. Thus, the detection techniques require an adaptive learning method to increases the performance level that is possible through machine learning.

Machine learning is based on artificial intelligence, which uses the mathematical method of statistical analysis to predict the desired output. It has the ability to learn from the data sets without explicit programming. The method used for implementing the required needs and applications is based on the type of learning approach. The main agenda is “to learn and improve” system performance with maximum efficiency. The learning mechanism is incorporated by training the system to learn from the datasets by themselves. This includes different stages like the extraction of the pattern from data sets to provide an optimized result in the adaptive environment. The use of machine learning in threat detection helps to identify the occurrence of threats with higher accuracy. It also effectively deals with the detection and mitigation of threats.

CYBER THREATS

In the digital revolution, everything is exercised through mobile devices and other electronic gadgets for sharing and accessing of resources with anonymous hazards. The scaling of valuable resources is calibrated based on the information prioritized by the user on their own standard. Even the lowest scaling data must be secured from the malicious act of penetration. The attack can be either active or passive which is used to obtain the desired information from the victim. To avoid such problems, a defensing mechanism is needed to safeguard the resources from invaders.

In order to provide security, a certain validation measure is necessary to protect the user data from the intruder. This includes the penetration process like detecting the vulnerable spots by various attacking techniques in order to get a higher success rate. They target initially at the network set up to analyze to