Chapter 35
Data Mining Analytics for Crime Security Investigation and Intrusion Detection

Boutheina Fessi
University of Carthage, Tunisia

Yacine Djemaiel
University of Carthage, Tunisia

Noureddine Boudriga
University of Carthage, Tunisia

ABSTRACT

This chapter provides a review about the usefulness of applying data mining techniques to detect intrusion within dynamic environments and its contribution in digital investigation. Numerous applications and models are described based on data mining analytics. The chapter addresses also different requirements that should be fulfilled to efficiently perform cyber-crime investigation based on data mining analytics. It states, at the end, future research directions related to cyber-crime investigation that could be investigated and presents new trends of data mining techniques that deal with big data to detect attacks.

INTRODUCTION

The continuous increase of the information streams and the dynamic feature of the environment, where the enterprise operates, could led to the emergence of new kinds of attacks that threat its information system. In fact, distributed and cyber attacks may be launched from different locations and targeted many sources, creating consequently a need to perform network data analysis from several networks locations.

A set of techniques and models are applied to mitigate these attacks but unfortunately they do not provide accurate protection. Therefore, novel measures and tools should be set up to prevent and secure these systems considering the high performance of computers, the newly smart attacks and the rising of vulnerabilities from inside and outside the information systems. Furthermore, tracing back the attack is

DOI: 10.4018/978-1-5225-9866-4.ch035

an important task to perform since it determines the intruder identity and source, and provides then the appropriate response to counter the detected attack.

Data mining techniques are a set of techniques that prove their effectiveness to cope with the cited issues. They are applied in several fields and implement different tasks. They could be performed in concert to make better detection and their principal aim is the extraction of knowledge from data which is tightly necessary when performing data collection and detection.

As it is mentioned in Figure 1, these techniques are used during the security investigation process that is performed within the enterprise. This latter is subjected to several factors that could affect its security, despite the existing policies and security tools. The investigation process is thus performed to efficiently detect and track the attacks that could harm its safety. It is based on data mining analytics, which deal with huge amounts of data and could perform several tasks related to cleaning, classifying and examining collected data.

The proposed chapter aims at presenting the harnessing of data mining analytics to crime security investigation and intrusion detection in company's communication networks. Numerous applications and models are described based on these analytics. The chapter also provides a review about the usefulness of applying data mining techniques to detect intrusion within dynamic environments, where the management of huge amounts of data is unavoidable. A set of challenges are thus identified when dealing with big data, including the detection and the tracing back of the attack if the information system is flooded by real time data. In addition, two cases studies related to medical and crime investigation are detailed showing the use of data mining techniques for the identification of attack scenarios.

Figure 1. Deployment of data mining techniques into enterprise investigation process