Abstract

iMedPub Journals
http://www.imedpub.com

American Journal of Computer Science and Information Technology

2021
Vol 19. S3

Data Fusion Based on Big Data Techniques in Intrusion Detection Context

Farah Jemili,
University of Sousse, Tunisia

Abstract

Intrusion detection has been the subject of numerous studies in industry and academia, but cybersecurity analysts still want a greater accuracy and comprehensive threat analysis to secure their systems in cyberspace. Improvements to intrusion detection could be achieved by adopting a more comprehensive approach in monitoring security events from many heterogeneous sources. Merging security events from heterogeneous sources can offer a more holistic view and a better knowledge of the cyber threat situation. A problem with this approach is that at present even a single event source (for example, network traffic) can encounter big data challenges when it is considered alone. Attempts to use more heterogeneous data sources poses an even greater challenge for big data. Big Data Technologies for Intrusion Detection can help solve these heterogeneous data Problems.

In this study, Big Data techniques are used to merge and clean the massive data in order to improve the intrusion detection performance. Our approach includes the pre-processing of data and the combination of many datasets into a single one. The experimental results show effectiveness of our approach in terms of accuracy and detection rate and prove that data fusion based on Big Data techniques can help achieve better results in Intrusion Detection context.

Key words: Data Fusion, Big Data Technique, Intrusion detection

Biography

Farah JEMILI received the Engineer degree in Computer Science in 2002 and the Ph.D degree in 2010. She is currently Assistant Professor at Higher Institute of Computer Science and Telecom of Hammam Sousse (ISITCOM), University of Sousse, Tunisia. She is a senior Researcher at MARS Laboratory (ISITCOM –Tunisia). Her research interests include Artificial Intelligence, Cyber Security, Big Data Analysis, Cloud Computing and Distributed Systems. She served as reviewer for many international conferences and journals. She has many publications; 6 book chapters, 5 journal publications and more than 15 conference papers.