World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:14, No:06, 2020

Intrusion Detection Based on Graph Oriented Big Data Analytics

Authors : Ahlem Abid, Farah Jemili

Abstract : Intrusion detection has been the subject of numerous studies in industry and academia, but cyber security analysts always want greater precision and global threat analysis to secure their systems in cyberspace. To improve intrusion detection system, the visualisation of the security events in form of graphs and diagrams is important to improve the accuracy of alerts. In this paper, we propose an approach of an IDS based on cloud computing, big data technique and using a machine learning graph algorithm which can detect in real time different attacks as early as possible. We use the MAWILab intrusion detection dataset . We choose Microsoft Azure as a unified cloud environment to load our dataset on. We implement the k2 algorithm which is a graphical machine learning algorithm to classify attacks. Our system showed a good performance due to the graphical machine learning algorithm and spark structured streaming engine.

Keywords : Apache Spark Streaming, Graph, Intrusion detection, k2 algorithm, Machine Learning, MAWILab, Microsoft Azure Cloud
Conference Title : ICCSIE 2020 : International Conference on Computer Science and Information Engineering
Conference Location : New York, United States
Conference Dates : June 04-05, 2020