World Academy of Science, Engineering and Technology
International Journal of Electrical and Information Engineering
Vol:13, No:10, 2019

Design of an Ensemble Learning Behavior Anomaly Detection Framework

Authors : Abdoulaye Diop, Nahid Emad, Thierry Winter, Mohamed Hilia

Abstract : Data assets protection is a crucial issue in the cybersecurity field. Companies use logical access control tools to vault their information assets and protect them against external threats, but they lack solutions to counter insider threats. Nowadays, insider threats are the most significant concern of security analysts. They are mainly individuals with legitimate access to companies information systems, which use their rights with malicious intents. In several fields, behavior anomaly detection is the method used by cyber specialists to counter the threats of user malicious activities effectively. In this paper, we present the step toward the construction of a user and entity behavior analysis framework by proposing a behavior anomaly detection model. This model combines machine learning classification techniques and graph-based methods, relying on linear algebra and parallel computing techniques. We show the utility of an ensemble learning approach in this context. We present some detection methods tests results on an representative access control dataset. The use of some explored classifiers gives results up to 99% of accuracy.

Keywords : cybersecurity, data protection, access control, insider threat, user behavior analysis, ensemble learning, high performance computing
Conference Title : ICISS 2019 : International Conference on Information Systems Security
Conference Location : Paris, France
Conference Dates : October 29-30, 2019