عمادة البحث العلمي
Deanship of Academic Research

الإنتاج العلمي لمركز بحوث علوم الحاسب والمعلومات

VISION رؤية 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

A Comparison of Re-Sampling Techniques for Detection of Multi-Step Attacks on Deep Learning Models

Authors	Muhammad Hassan Jamal, Naila Naz, Muazzam A. Khan Khattak, Faisal Saeed, Saad Nasser Altamimi, And Sultan Noman Qasem
Publication Year	2023
Grant Number	IMSIU-RG23052.
DOI link	https://doi.org/10.1109/ACCESS.2023.3332512

Abstract: The increasing dependence on data analytics and artificial intelligence (AI) methodologies across various domains has prompted the emergence of apprehensions over data security and integrity. There exists a consensus among scholars and experts that the identification and mitigation of Multi-step attacks pose significant challenges due to the intricate nature of the diverse approaches utilized. This study aims to address the issue of imbalanced datasets within the domain of Multi-step attack detection. To achieve this objective, the research explores three distinct re-sampling strategies, namely over-sampling, undersampling, and hybrid re-sampling techniques. The study offers a comprehensive assessment of several re-sampling techniques utilized in the detection of Multi-step attacks on deep learning (DL) models. The efficacy of the solution is evaluated using a Multi-step cyber attack dataset that emulates attacks across six attack classes. Furthermore, the performance of several re-sampling approaches with numerous traditional machine learning (ML) and deep learning (DL) models are compared, based on performance metrics such as accuracy, precision, recall, F-1 score, and G-mean. In contrast to preliminary studies, the research focuses on Multi-step attack detection. The results indicate that the combination of Convolutional Neural Networks (CNN) with Deep Belief Networks (DBN), Long Short-Term Memory (LSTM), and Recurrent Neural Networks (RNN) provides optimal results as compared to standalone ML/DL models. Moreover, the results also depict that SMOTEENN, a hybrid re-sampling technique, demonstrates superior effectiveness in enhancing detection performance across various models and evaluation metrics. The findings indicate the significance of appropriate re-sampling techniques to improve the efficacy of Multi-step attack detection on DL models.