World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

A Deep Learning Approach to Online Social Network Account Compromisation

Authors : Edward K. Boahen, Brunel E. Bouya-Moko, Changda Wang

Abstract : The major threat to online social network (OSN) users is account compromisation. Spammers now spread malicious messages by exploiting the trust relationship established between account owners and their friends. The challenge in detecting a compromised account by service providers is validating the trusted relationship established between the account owners, their friends, and the spammers. Another challenge is the increase in required human interaction with the feature selection. Research available on supervised learning (machine learning) has limitations with the feature selection and accounts that cannot be profiled, like application programming interface (API). Therefore, this paper discusses the various behaviours of the OSN users and the current approaches in detecting a compromised OSN account, emphasizing its limitations and challenges. We propose a deep learning approach that addresses and resolve the constraints faced by the previous schemes. We detailed our proposed optimized nonsymmetric deep auto-encoder (OPT_NDAE) for unsupervised feature learning, which reduces the required human interaction levels in the selection and extraction of features. We evaluated our proposed classifier using the NSL-KDD and KDDCUP'99 datasets in a graphical user interface enabled Weka application. The results obtained indicate that our proposed approach outperformed most of the traditional schemes in OSN compromised account detection with an accuracy rate of 99.86%.

Keywords : computer security, network security, online social network, account compromisation
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020