Detection of phishing websites using machine learning approaches

ABSTRACT

As the world responded to the Coronavirus Disease 2019 (COVID-19) pandemic in 2020, digital operations became more important, and people started to depend on new initiatives such as the cloud and mobile infrastructure. Consequently, the number of cyberattacks such as phishing has increased. Phishing websites can be detected using machine learning by classifying the websites into legitimate or illegitimate websites. The purpose of the study is to conduct a mini-review of the existing techniques and implement experiments to detect whether a website is malicious or not. The dataset consists of 11,055 observations and 32 variables. Three supervised learning models are implemented in this study: Decision Tree, K-Nearest Neighbour (KNN), and Random Forest. The three algorithms are chosen because it provides a better understanding and more suitable for the dataset. Based on the experiments undertaken, the result shows Decision Tree has an accuracy of 91.16% which is the lowest compared to the other models, 97.6% for the KNN model which is the highest among all the models and 94.44% accuracy for the Random Forest model. Through comparisons between the three models, KNN was the prime candidate for the best model considering that it has the highest accuracy. However, Random Forest is deemed more suitable for the dataset even though the accuracy is lesser because of the lowest false-negative value than the other models. The experiments can be further investigated with different datasets and models for comparative analysis.