MIDI 2024 Conference

Uncovering Phishing URLs to mitigate cyber threats using Machine Learning Models

Abstract

In this research study, we provide a comparative analysis of 12 machine learning models, which are categorized as Standalone models, Ensemble models, and Deep Learning models and then select the best model to develop a framework that automatically detects phishing URLs so that users can safely browse without any delay. We gathered 600,000 URLs as a dataset of phishing and genuine URLs, and extracted 19 elements from the URLs, including Have IP, Have At, URL Length, URL profundity, Non-standard twofold slice, https domain, shortened URL, Dash Count, Has keywords, DNS Record, Comb 5y interest, Blacklisted Domain, Domain age, Domain active, iFrame, Mouse Over, Right click, Web Forwards, and Label. We then trained different AI models on this dataset, including standalone models like decision Trees, KNN, Logistic Regression and Naive Bayes and ensemble models like Random Forests, XGBoost, AdaBoost and Hard Voting and Deep learning models like ANN, LSTM, GRU and CNN. We evaluated the performance metrics such as accuracy, recall, precision, train time and prediction time on these models. Out of the selected categories of standalone models, ensemble models and deep learning models, we observed that ensemble models appear to have the best overall performance in terms of accuracy and prediction time and among the ensemble models the XGBoost model has the highest accuracy of 95.073% and the lowest prediction time of 0.173 seconds. Moreover, XGBoost produced the lowest number of false positives at 3000 URLs out of 600,000 URLs. Hence, for our proposed phish detection framework, we selected XGBoost as the final model.