Abstract

Social network services (SNSs) are increasing popular. Now a day’s most of the people in all over the world use Facebook, twitter for sharing their ideas. Though suspicious users collectively use by them to embed to harmful activities that may be tricky in securing user’s personal information and data. This is challenge for social networks to rectify this type of security breach. The social networks or community websites must be able to identify phishing and suspicious urls.

Machine learning techniques are proved an efficient tool in classifying benign and the suspicious urls from the set of many urls most of the solutions for training the classification models that supported all totally different sorts of feature sets. However, the most of the solutions does not provide good results as we expect from them on the basis of performance, behavior and some other criteria.

In this study, a feature set is presented that combines the features of traditional heuristics and
social networking. Furthermore, a suspicious URL identification system for use in social network environments is proposed which is based on comparative study of three algorithms named as Bayesian classification, KNN, SVM. The experimental results indicate that the proposed approach achieves a high detection rate.

References

16. Irani, Danesh, Marco Balduzzi, Davide Balzarotti, Engin Kirda, and Calton Pu. "Reverse social engineering attacks in online social networks." In Detection of intrusions and malware,


Index Terms
Computer Science Software Engineering

Keywords
ON-Line Social Networks, Suspicious URLS, Naive Bayesian Classification, KNN, SVM, Machine Learning,