Phishing Website Detection using Associative Classifiers

Divya V[1], Vivitha Vijay[2]

[1][2]Assistant Professor, Department of Computer Science and Engineering, Sri Vellappally Natesan College of Engineering, Kerala, India

Abstract

Phishing is a criminal technique employing both social engineering and technical subterfuge to steal consumer's personal identity data and financial account credential. The aim of the phishing website is to steal the victim's personal information by visiting and surfing a fake webpage that looks like a true one of a legitimate bank or company and asks the victim to enter personal information such as their username, account number, password, credit card number, etc. The main goal is to investigate the potential use of automated data mining techniques in detecting the complex problem of phishing websites in order to help all users from being deceived or hacked by stealing their personal information and passwords leading to catastrophic consequences. Experimentations against phishing data sets and using different common associative classification algorithms (MCAR and CBA) and traditional learning approaches have been conducted with reference to classification accuracy.

Keywords: Phishing Websites, Data Mining, Associative Classification, Machine Learning.