Phishing Prediction in e-banking Using Data Mining Techniques

M. Govindaraj [1] and A.L. Hanees[2]*

Department ofComputer Science & Engineering, Bharathidasan University, India.
*Department ofMathematics and Computer Science, South Eastern University ofSri Lanka,
Corresponding Author: alhanees@seu.ac.lk

Phishing is a form of electronic identity stealing in which a mixture of social engineering and web site spoofing techniques is used to trap a user into useful confidential information with financially viable value in e-banking. In detecting and identifying ebanking phishing websites, Classification Data Mining (DM) Techniques can be a very useful tool. In this paper, we considered and implemented six different classification algorithm and techniques to extract the phishing training data sets criteria to classify their legitimacy in e-banking. We also compared their performances, accuracy, number of rules generated and speed. The experimental results demonstrated the feasibility of using Associative Classification techniques in real e-banking applications and its better performance as compared to other traditional classification algorithms. We present a novel approach to overcome the difficulty and complexity in detecting and predicting ebanking phishing website. We proposed an intelligent resilient and effective model that is based on using association and classification Data Mining algorithms. These algorithms were used to characterize and identify all the factors and rules in order to classify the phishing website and the relationship that correlate them with each other. The rules generated from the associative classification model showed the relationship between some important characteristics like URL and Domain Identity and Security and Encryption criteria in the final phishing detection rate.

Key Words: Classification, Association, Data mining