ABSTRACT:

With the development of e-commerce transaction, phishers and other cybercriminals are taking advantage and making the online platform insecure by triggering severe threats to users and industries as well as intimidating worldwide safety and economy. Currently, phishers are regularly developing different means for tempting user to expose their delicate facts. In order to elude falling target to phishers, it is essential to implement a phishing detection algorithm. Phishing is a way to deceive people in believing that the URL which they are visiting is genuine. Once the user establishes his/her trust on the website they enter their personal credentials like login password or account number etc. Attacker sends spam emails and develops identical websites which resembles the original websites and affects fields such as online business, e-commerce, digital marketing and banking. This paper aims to develop a system which identifies phishing URL with various machine learning methods and comparing it with hybrid stacking model to identify the approach which provides maximum accuracy rate and time effectively. In the proposed research work, different Machine Learning algorithms like Logistic Regression are compared with ensemble algorithms like Ad boost and Gradient boost. The research outcome shows that the proposed Stacking Classifier results 85.6 percentage of accuracy. The classifiers which provide better phishing predictions outcome are already available. However, with our comparative survey shows that the hybrid approach improves the accuracy prediction rate of phishing websites.