Literature survey

WEB PHISHING DETECTION

S.NO	TITLE OF THE JOURNAL	YEAR OF PUBLICATION	INFERENCE
1.	Detection of phishing websites using an efficient feature-based machine learning framework	2018	In this, they have classified extracted features into three categories such as URL Obfuscation features, Third-Party-based features, Hyperlink-based features. Moreover, the proposed technique gives 99.55% accuracy. Drawback of this is that as this model uses third party features, classification of websites depends on the speed of third-party services. Also this model purely depends on the quality and quantity of the training set and Broken links feature extraction has a limitation of more execution time for the websites with more number of links.
2.	Finding effective classifier for malicious URL detection	2018	In this they have combined statistical analysis of URL with machine learning technique to get a result that is more accurate for classification of malicious URLs. Also they have compared six machine-learning algorithms to verify the effectiveness of the proposed algorithm which gives 99.7% precision with false positive rate less than 0.4%.

3.	Detecting Phishing Websites Using Rule-Based Classification Algorithm	2018	They have proposed rule based classification techniques for phishing website detection. They have concluded that association classification algorithms are better than any other algorithms because of their simple rule transformation. They achieved 92.67% accuracy by extracting 16 features but this is not up to mark so the proposed algorithm can be enhanced for efficient detection rate.
4.	A Hybrid Model to Detect Phishing-Sites using Supervised Learning Algorithms	2016	In this paper, a proposed model was carried out in two phases. In phase 1,they individually perform classification techniques, and select the best three models based on high accuracy and other performance criteria. While in phase 2, they further combined each individual model with the best three models and made a hybrid model that gives better accuracy than individual models. They achieved 97.75% accuracy on the testing dataset. There is limitation of this model that it requires more time to build hybrid model

5.	A Framework for Auto-Detection of Phishing Websites	2017	For phishing websites, machine-learning data can be created using this framework. In this, they have used reduced features set and using python for building query .They build a large labeled dataset and analyze several machine-learning classifiers against this dataset .Analysis of this gives very good accuracy using machine-learning classifiers. These analyses how long it takes to train the model.