TITLE	AUTHOR	YEAR	TECHNIQUES	FINDINGS
Detection of Phishing Websites by Using Machine Learning-Based URL Analysis	Mehmet Korkmaz, Ozgur KoraySahingoz, BanuDiri.	2020	XGBOOST ,RF , LR ,KNN,SVM,DTANN ,NB	A machine learning-based phishing detection system by using eight different algorithms to analyze the URLs, and three different datasets to compare the results with other works. The experimental results depict that the proposed models have an outstanding performance with a success rate.
A Deep Learning-Based Framework for Phishing Website Detection	Lizhen Tang And Qusay H. Mahmoud	2021	RNN-GRU, web browser extension.	The author briefed that they have implemented the framework as a browser plug-in capable of determining whether there is a phishing risk in real-time when the user visits a web page and gives a warning message.It combines multiple strategies to improve accuracy, reduce false alarm rates, and reduce calculation time, including whitelist filtering, blacklist interception, and machine learning (ML) prediction.
Detection of Phishing Websites from URLs by using Classification Techniques on WEKA	BuketGeyik, Kubra Erensoy, EmreKocyigit	2021	machine learning, classification algorithms, phishing detection, cybersecurity	The anti-phishing method has been developed by detecting the attacks made with the technologies used. we combined the websites used by phishing attacks into a dataset, then we obtained some results using 4 classification algorithms with this dataset.
Real Time Detection of Phishing Websites	Abdulghani Ali Ahmed, Nurul Amirah Abdullah	2016	URL; Real Time Model; Phishing Detection	A detection technique of phishing websites based on checking Uniform Resources Locators (URLs) of web pages. The proposed solution is able to distinguish between the legitimate web page and fake web page by checking the Uniform Resources Locators (URLs) of suspected web pages. URLs are inspected based on particular characteristics to check the phishing web pages. The detected attacks are reported for prevention. The performance of the proposed solution is evaluated using Phish tank and Yahoo directory datasets.

Phishing URL Detection: A Real-Case Scenario Through Login URLs	manuel sánchez-paniagua , eduardo fidalgo fernández , enrique alegre , wesam al-nabki , and víctor gonzález-castro	2022	machine learning and deep learning approaches, cybercrime, phishing detection, url.	The list provided on that website only contains the domain names, extracted the complete URL. To reach the login page from a website,It used the Selenium web driver and Python, checking buttons or links that could lead to the login form web page.Once we found the presumptive login and inspected if the form had a password field in order to confirm whether it was a login form. Otherwise, it was not added to the dataset. In this, collected reported phishing URLs from Phishtank.
A Novel Machine Learning Approach to Detect Phishing Websites	Ishant Tyagi, Jatin Shad, Shubham Sharma, Siddharth Gaur, Gagandeep Kaur	2018	Decision Tree, Random Forest, Gradient Boosting , Generalized Linear Model, prediction for a new URL.	In this technique ,they determined most targeted brand names and their legit URL via Google and their real phishing URLs from PhishTank website. Those extracted using python and used for prediction for a new URL. Input URL, Extract 30 features of URL, Use these features for predictive analysis,It checks whether it obtains positive or negative output,if negative it notifies the user that the website is phishing otherwise Notify the user that the website is safe
Detection of Phishing Websites using Machine Learning	Abdul Razaque, Mohamed Ben Haj Frej, Dauren Sabyrov, Aidana Shaikhyn, Fathi Amsaad, Ahmed Oun	2020	Phishing website detection, 'Anti-phishing and Authenticity Checker', CPU Consumption,	Features are inspected using a set of rules to select URLs ofphishing webpages from the URLs of dangerous websites.The detecting process includes:Using a blacklist database, which contains URLs of all phishing websites. Using the IP Address: If an IP address is in the URL, such as "http://125.98.3.123/fake.html", users can be sure that someone is trying to steal their sensitive personal information. Using mail/mail-to attributes: if these attributes are found in the URL, users can be sure that someone wants to steal their information

Detecting Phishing Websites Using Machine Learning	Amani Alswailem, Bashayr Alabdullah, Norah Alrumayh, Dr.Aram Alsedrani	2019	Random forest, URL, browser extension, machine learning, phishing websites, phishing features.	The author briefed , they offer an intelligent system for detecting phishing websites. The system acts as an additional functionality to an internet browser that automatically notifies the user when it detects a phishing website. Forest technique due to its good performance in classification. Our focus is to pursue a higher performance classifier by studying the features of phishing website and choose the better combination of them to train the classifier. As a result, this paper conclude with accuracy and combination of 26 features.
Prediction of Phishing Website for e-Banking Using Data Mining Techniques	Nemmi Swathi, C Maddilety	2021	Phishing, Fuzzy Logic, Data Mining, six different common DM classification algorithms (C4.5, JRip, PART, PRISM, CBA and MCAR).	The motivation behind this study is to create a resilient and effective method that uses Data Mining algorithms and tools to detect e-banking phishing websites in an Artificial Intelligent technique. In this paper, they managed to gather *27 phishing features* and indicators and clustered them into *six Criteria.* Phish Checker application also can be upgraded into the web phone application in detecting phishing on the mobile platform.
Phishing Website Detection using Machine Learning Algorithms	Rishikesh Mahajan, Irfan Siddavatam	2018	Phishing attack, Machine learning	The author deals with machine learning technology for detection of phishing URLs by extracting and analyzing various features of legitimate and phishing URLs. Decision Tree, random forest and Support vector machine algorithms are used to detect phishing websites. Aim of the paper is to detect phishing URLs as well as narrow down to best machine learning algorithm by comparing accuracy rate, false positive and false negative rate of each algorithm.