WEB PHISHING DETECTION:

PROBLEM STATEMENT:

Phishing is the fraudulent attempt to obtain sensitive information such as username, password, bank account details, and credit card details for malicious use, Phishing frauds might be the most popular cybercrime used today. There are various domains where phishing attack can occur like online payment sector. webmail and financial institution. file hosting or cloud storage and many others. The webmail and online payment sector were targeted by phishing more than in any other industry sector. Several anti-phishing techniques are there such as blacklist, heuristic, visual similarity and machine learning. From this, blacklist approach is commonly used because it is easy to use and implement bat it fails to detect new phishing attacks, Machine Learning is efficient technique to detect phishing. It also removes drawback of existing approach. We perform detailed Literature survey and proposed new approach to detect phishing website by features extraction and machine learning algorithm.

Who does the problem affect?	Phishing is a type of social engineering attack often used to steal user data including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening a mail, instant message or text message.
What are the boundaries of the problem?	When we click on the malicious link
What is the issue?	Money loss, stealing of important data
When does the issue occur?	When we unknowingly click on the malicious links and give our personal and card details
Where does the issue occur?	On websites
Why is it important that we fix the problem?	To secure our personal details from the stranger
What solution to solve this issue?	Identify the malicious website Warn the user about the attack Block the website.
What methodology is used to solve the issue?	Machine learning based ensemble techniques can be used to increase the prediction accuracy and we can make use of the algorithm for detecting the malicious website