Proposed Solution :

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Internet has dominated the world by dragging half of the world's population exponentially into the cyber world. With the booming of internet transactions, cybercrimes rapidly increased and with anonymity presented by the internet, Hackers attempt to trap the end-users through various forms such as phishing, SQL injection, malware, man-in-the-middle, domain name system tunnelling, ransomware, web trojan, and so on. Among all these attacks, phishing reports to be the most deceiving attack. The aim is to classification of a phishing website with the aid of various machine learning techniques to achieve maximum accuracy and concise model.
2.	Idea / Solution description	Detection and prevention of phishing websites endure measure continuously a major space for analysis. There are different types of phishing techniques that offer torrential and essential ways that offer attackers to penetrate the data of people and organizations. Uniform resource locator URLs play a vital role in a phishing attack. Uniform resource locator has a vulnerability of redirecting the pages which could redirect to the legitimate website or the phishing site. Different techniques in making phishing sites are emerging day by day. This is the motivation for finding the phishing sites.
3.	Novelty / Uniqueness	We are to use a minimum of 5 different models to find the accuracy from the given data set and among them, the best accuracy delivering model is chosen. We have planned to include deep learning algorithm to get the best accuracy. Then the chosen model is used to build a website which detects and finds phishing websites.
4.	Social Impact / Customer Satisfaction	Sometimes a phishing scam will install malware (malicious software) on a user's device. Once infected scammers have access to files and can track user behaviour. By accessing these files and spying on employee's digital movements, cyber criminals can actively steal important company data. Such instances can be avoided by detecting the scams beforehand.
5.	Business Model (Revenue Model)	This "Web Phishing Detection" model with the best accuracy can interest many corporates' attention. It can be sold directly or it can be integrated along with an anti-virus software to deliver a complete package of security. This can be made into an application or a website to serve the web users for a fee varying to their term plans.
6.	Scalability of the Solution	The model can be used in many ways and it can further be made better as new data can be added and tested. It can be made into and application for various devices and operating systems. It can be integrated along with an anti-virus software. New models can be tested with the current data and the models can be updated to improve accuracy.