Project Initialization and Planning Phase

Date	06-06-2024
Team ID	740031
Project Name	Detection of phising websites from URLS
Maximum Marks	3 Marks

Define Problem Statements :

Detecting phishing websites from URLs is a crucial task in cybersecurity. To tackle this challenge, several problem statements can be defined. Firstly, a classification problem can be formulated, where a system is designed to categorize URLs as phishing or legitimate based on features extracted from the URL itself. Another approach is anomaly detection, which involves identifying URLs that significantly deviate from legitimate URL patterns, indicating potential phishing attempts. Additionally, a predictive model can be built using historical data and machine learning algorithms to predict the likelihood of a URL being phishing. Feature extraction is also a key problem statement, where relevant features such as domain, TLD, length, and special characters are extracted from URLs to distinguish phishing URLs from legitimate ones. Real-time detection is another crucial problem statement, which involves detecting phishing URLs promptly to enable immediate warnings or blocking of malicious sites. Furthermore, context-aware detection considers additional context like user behavior and browser history to improve detection accuracy. Finally, zero-day detection aims to identify previously unknown phishing URLs without relying on existing blacklists or signatures. By defining these problem statements, effective phishing detection systems can be developed to enhance online security and protect users from cyber threats.