Ideation phase
Literature Survey

Date	19 september 2022
Team ID	PNT2022TMID24960
Project Name	Web Phishing Detection
Maximum Marks	4 marks

WEB PHISHING DETECTION

ABSTRACT

Phishing is an attack against internet users that causes them to reveal their info using fake websites. The goal of the fake website is to steal information such as username,password and other sensitive information.

Machine Learning is a powerful tool used to combat spoofing attacks. This report covers machine learning applied science to detect fake URLs.

INTRODUCTION

The internet plays an important role today. It has many features. It shares everything quickly and with a high speed. It also have a lots of risk when an user use online platform. Then they place on popular websites or sent to user emails.

LITERATURE SURVEY

1. Web phishing detection using deep learning framework

Despite numerous research efforts, phishing attacks remain prevalent and effective in unsuspecting users to reveal sensitive information including social security numbers. In this project we propose Phishing a new feature rich machine learning framework to detect phishing webpages. These features capture various characteristics of legitimate web applications as well as their underlying web infrastructures. In our experiments, Phishing achieved 91.6% accuracy with 8.4% false positive rate on a dataset containing unique phishing instances using machine learning framework.

2. Spam detection using machine learning techniques

Nowadays email are use in almost every field , from business to education. Emails has two subcategories, ham and spam. Also call junk email is a type of email that can be use to harm any user by stealing valuable info. Spam detection is significant and enormous problem for IOT service providers nowadays. Preventing and filtering is essential approaches. Several machine learning and deep learning technique have been use to get comprehensive comparison of these technique to get base on accuracy and precision are discuss.

3. Machine learning based phishing detection from URL's

In the recent years, advancements in internet and cloud applied science have led to a significant increase in electronic trading in which consumers make online purchases and transactions. Phising is one of the similar attacks that trick users to access malicious content and gain their info.

In terms of website interface and uniform resource locator most phishing websites, such as blacklist , heuristic have been suggest. However, due to the inefficient security applied science, there is an exponential increase in the number of victims.

The anonymous and uncontrollable framework of the internet is more vulnerable to phishing attacks. A recurrent neural network method is employee to detect phishing URL. Researcher evaluated the proposed with 7900 malicious and 5800 legitimate sites, respectively. The experiments outcome shows the better performance than the recent approaches in malicious URL detection.

Conclusion

This paper aims to enhance detection method to detect phishing websites using machine learning technology. We achieved 97.14% detection accuracy using random forest algorithm with lowest false positive rate. Also result shows that classifiers give better performance when we used more data as training data.