WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

DETECTION AND PREVENTION OF PHISHING USING MACHINE LEARNING

Harshal Mali[a], Parth Chavan[a],Aditya Dhotre[a], and Aryan Habib[a] Naresh Kamble[b]

[a]*Student, Sanjay Ghodawat Polytechnic, Atigre MH 412105, India.*
[b]*Faculty, Sanjay Ghodawat Polytechnic, Atigre MH 412105, India.*

ABSTRACT

Naive browser users have no idea what goes on behind the scenes of a page. Users may be tricked into disclosing their credentials or downloading malicious software. Our goal for the proposed project is to create a Chrome plugin that acts as a middleman between users and hazardous websites, minimizing the likelihood of consumers falling to them. Furthermore, it is impossible to collect all dangerous content because it is continually changing. We're taking steps to combat this.

Keywords*: Machine learning, Chrome, Extension, Phishing, Malicious, URL*

1. INTRODUCTION

Different types of web threats can result in identity theft, the theft of private information, financial loss, and the loss of customer trust in online banking and e-commerce. As a result, the internet's suitability for commercial transactions is questioned. Phishing is a type of web threat that is defined as the art of impersonating a legitimate company's website.

Fraudsters create phishing websites in order to imitate the web pages of legitimate websites. These phishing websites, which look similar to legitimate ones, defraud honest internet users. Because the number of phishing websites is growing by the day, it will become a serious problem, even for experienced computer security and internet users.

1.1 Objective of project

1. Detect and eliminate risk of phishing.
2. Detect website spoofing..
3. Overcome the drawbacks of existing solutions which fails to serve the purpose.
4. Implement Real time URL classification using Phish tank

1.2 Approaches

Two approaches are used in **recognizing** phishing websites to distinguish between honest and phishing websites. The first determines whether the requested URL is on any blacklists by comparing it to those on that list.

The second strategy involves using meta-heuristic approaches to collect a large number of characteristics from a website in order to classify it as authentic or phishing.

2. METHODOLOGY

Machine learning technology was used by researchers to detect dangerous URLs.

Based on statistical features, machine learning builds the prediction model and classifies a URL as harmful or benign. To extract the characteristics, this approach attempts to examine URLs and their respective websites or web page information. This method's retrieved characteristics are frequently separated into two types: static features and dynamic features. Literature extracts lexical information from URL strings, host information, and, on occasion, HTML and JavaScript content. The support vector machine (SVM) is used to detect a variety of network traffic-related characteristics extracted from URLs in the literature. Three feature processing strategies are proposed in the literature to optimize the classification effect.\\

While the approaches described above have demonstrated high performance, they do have significant limitations. Traditional machine learning-based detection approaches sometimes need manually extracting characteristics. Attackers can evade detection by constructing these traits, making it harder to maintain the detection system based on classical machine learning. Furthermore, when detecting fraudulent URLs on a broad scale, a trained model may lose some essential information from the URL.

2.1 Signature based Malicious URL Detection

Studies on malicious URL detection using the signature sets had been investigated and applied long time ago. Most of these studies often use lists of known malicious URLs. Whenever a new URL is accessed, a database query is executed. If the URL is blacklisted, it is considered as malicious, and then, a warning will be generated; otherwise URLs will be considered as safe. The main disadvantage of this approach is that it will be very difficult to detect new malicious URLs that are not in the given list.

2.2 Machine Learning based Malicious URL Detection

There are three types of machine learning algorithms that can be applied on malicious URL detection methods, including supervised learning, unsupervised learning, and semi supervised learning. And the detection methods are based on URL behaviors. In, a number of malicious URL systems based on machine learning algorithms have been investigated. Those machine learing algorithms in- clude SVM, Logistic Regression, Nave Bayes, Decision Trees, Ensembles, Online Learning, etc.

3. IMPLEMENTATION OF PROJECT

1. Obtaining Dataset :

The dataset was obtained from the UCI - Machine Learning Repository which contains the Phishing Web Site Dataset. This dataset is composed of 11055 entries of websites which are classified as phishing and benign. These entries each have 30 features of the website used.

2. Feature Selection :

From the dataset, out of the 30 features present, it was infeasible to extract all the features. This is because many features used some standard databases which are not accessible to us. Also, extracting some of the features seemed not possible as they demanded the extraction of data from the server of the website, which is not possible. Hence, we narrowed down our dataset to contain 22 features.

3. Choosing Classification Algorithm

For classifying the URL entered, as either safe or malicious, we considered the following algorithms:

- The K-Nearest Neighbors (kNN) algorithm can be used to solve both classification and regression problems. However, it is mostly employed to solve categorization difficulties. The number of nearest neighbours we want to vote from is represented by the letter 'k' in the kNN method. This algorithm will search the training dataset for the closest k-samples when predicting for a new data sample.
- SVMs (Support Vector Machines) are supervised learning models that can be used for classification and regression. The SVM algorithm works with a dataset that has input samples separated into two classes, each with a label of 0 or 1. Finding a line or a plane, also known as a hy- perplane, that will most efficiently split the two classes is part of the process.

3.1 Phish tank

Phishing blacklists are a common defence tactic that aims to protect consumers against phishing attempts. These blacklists often comprise known phishing URLs, giving an access control list that is used to restrict people from visiting these risky websites. Google Safe Browsing (GSB), PhishTank (PT) https://phishtank.org/, and OpenPhish are three common phishing blacklists used nowadays (OP).

Challenges and solutions One of the most difficult aspects of our research was the paucity of phishing datasets. Despite the fact that several scientific pub- lications on phishing detection have been published, none of them have given the dataset that they utilised in their research. Another aspect that makes it difficult to discover an acceptable dataset is the lack of a common feature set for recording features of a phishing website. Some scholars thoroughly investigated and benchmarked the dataset we utilised in our study. Fortunately, the dataset's associated wiki includes a data description paper that details the data produc- tion methodologies used by the dataset's developers phishing-dataset. We have also incorporated code that pulls features of new phishing websites published by the PhishTank website in order to update our dataset with new phishing websites. The dataset comprises around 11,000 sample websites.The dataset's associated wiki contains a data description paper that goes over the data pro- duction methodologies used.

In this work, we assessed model performance using publicly accessible Phishing websites data sets from the UCI machine learning repository, as well as open source WEKA2 machine learning.

In this study, accuracy is used to check the performances of the classifiers

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FP} * 100 \quad (1)$$

4. RESULTS OF PROJECT

where TP, FP, TN and FN are number of true positives, false positives, true negatives and false negatives respectively. F-measure is also another performance measure and defined as follows:

$$F - measure = 2 * \frac{PrecisionxRecall}{Precision + Recall} \quad (2)$$

where

$$Precision = \frac{TP}{TP + FP} \quad (3)$$

$$Recall = \frac{TP}{TP + FN} \quad (4)$$

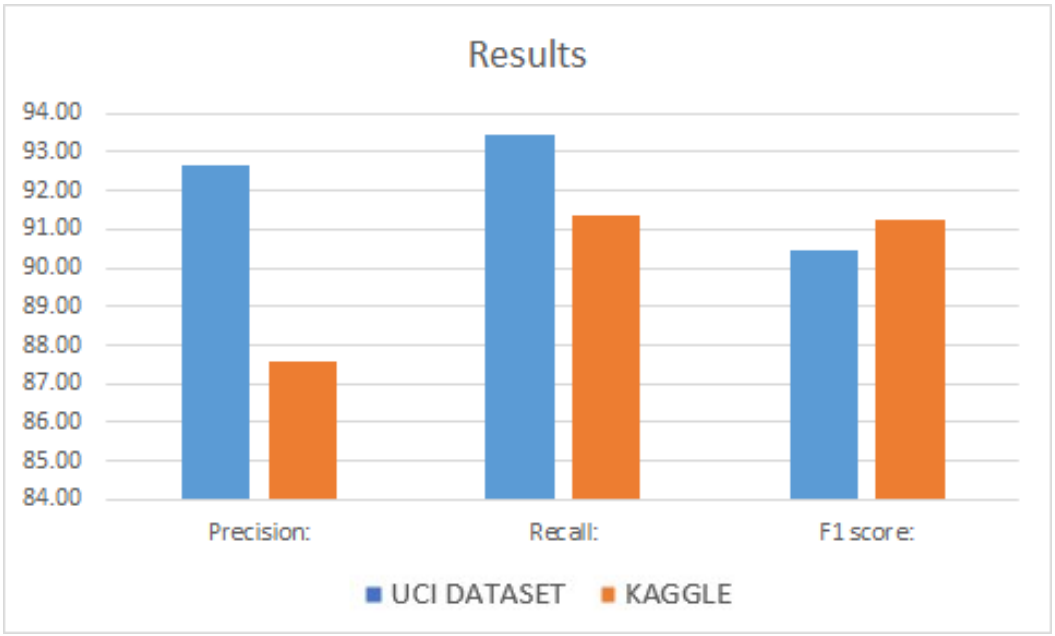

Fig 4.1 Result of comparing two datasets accuracy after training using Knn algorithm

5. CONCLUSION

A method for detecting malicious URLs using machine learning is presented in this paper. We do not use special attributes in this study, nor do we seek to cre- ate massive datasets to improve the system's accuracy, as many other traditional publications do. In this case, the combination of easy-to-calculate attributes and big data processing technologies to ensure the balance of the two factors is the system's processing time and accuracy. The findings of this study can be applied and implemented in information security technologies and systems. By com- bining this with a real-time phishing URL database, we will ensure the highest level of security for our users. It is worth noting that the combination of multiple classifiers does not always outperform the best individual classifier in the ensem- ble classifiers. The findings encourage future research to add more features to the dataset, which could improve the performance of these models; thus, it could combine machine learning models with other phishing detection techniques, such as List-Base methods, to achieve better performance. In addition, we will investi- gate the possibility of proposing and developing a new mechanism for extracting new features from the website in order to keep up with new phishing attack techniques.

REFERENCES

[1] Harshal Mali, Aditya Dhotre 'Detection and prevention of phishing using machine learning' Inter- national Journal of Research Publication and Reviews 2021

[2] Abdulhamit Subasi 'Intelligent Phishing Website Detection using Random Forest Classifier' 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)

[3] R. S. Rao and S. T. Ali, "A computer vision technique to detect phishing attacks," in 2015 Fifth International Conference on Communication Systems and Network Technologies, pp. 596–601, IEEE, 2015.

[4] UC Irvine Machine Learning Repository. https://archive.ics.uci.edu/ml/datasets. php

[5] Phishtank https://phishtank.org/