TEAM ID :PNT2022TMID3547

WEB PHISHING DETECTION

LITERATURE SURVEY

1. **URL-based Phishing Websites Detection via Machine Learning**

   2021 - IEEE - International Conference on Data Analytics for Business and Industry (ICDABI)

   Phishing is a social engineering cybersecurity attack that involves an attacker who provides a counterfeit piece of information that is hand-crafted skillfully to trick a user (human victim usually) to provide sensitive information to the attacker or to install malicious software on the victim's computing platform. The system developed in this paper for phishing websites is detected using URL addresses and solves binary classification problems where websites are classified into either authentic or phishing websites. The system utilized machine learning techniques such as shallow neural networks and decision trees to learn data patterns in websites URLs. The system has been evaluated on the Phishing Websites Dataset which includes small (balanced-class) and large (unbalanced-class) datasets. Aimed at improving the computational efficiency of our system by providing an optimized implementation using fast machine learning frameworks built using low-level programming languages.

2. **A Machine Learning Approach for URL Based Web Phishing Using Fuzzy Logic as Classifier**

   2019 International Conference on Communication and Electronics Systems (ICCES)

   Phishing is the major problem of the internet era. In this era of internet the security of our data in web is gaining an increasing importance. Phishing is one of the most harmful ways to unknowingly access the credential information like username, password or account number from the users. Users are not aware of this type of attack and later they will also become a part of the phishing attacks. It may be the losses of financial found, personal information, reputation of brand name or trust of brand. So the detection of phishing site is necessary. In this paper we design a framework of phishing detection using URL.

3. **Detecting Phishing Websites Using Machine Learning**

   2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)

   Phishing website is one of the internet security problems that target the human vulnerabilities rather than software vulnerabilities. It can be described as the process of attracting online users to obtain their sensitive information such as usernames and passwords. In this paper, we offer an intelligent system for detecting phishing websites. The system acts as an additional functionality to an internet browser as an extension that automatically notifies the user when it detects a phishing website. The system is based on a machine learning method, particularly supervised learning. We have selected the Random Forest technique due to its good performance in classification. Our focus is to pursue a higher performance classifier by

studying the features of phishing website and choose the better combination of them to train the classifier.

4. **A Methodical Overview on Detection, Identification and Proactive Prevention of Phishing Websites**

   2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV).

   This project is a natural way to deal with quality variables. It will present an approach to solving the fuzziness in the phishing website assessment and propose an accurate and smart model for detecting phishing websites. This phishing detection technique is based on fuzzy logic and machine learning algorithms in order to distinguish different factors on the phishing website. According to their study, for phishing identification with greater precision, a total of 30 characteristics and phishing site variables can also be used. A real-time phishing dataset is used which is downloaded from the UCI machine learning repository. This approach is based on smooth logic and machine learning algorithms that define various factors on the phishing website.

5. **Feature extraction and classification phishing websites based on URL**

   2015 IEEE Conference on Communications and Network Security (CNS)

   Phishing is a malicious form of online theft that aims at stealing users' personal information, such as online banking passwords, credit card numbers and other financial data. In the last decade, many users suffered monetary losses as a result of the increasing number of phishing attacks. The motivation of our study is to propose a safer framework for detecting phishing websites with high accuracy in less time.

The detection of phishing can be achieved by either increasing user awareness or using software based detection. Although there are several software detection techniques that address the problem of phishing detection, phishing has become more and more complicated and sophisticated, and can bypass the filter set by anti-phishing techniques. In this study, we extracted more URL features and analyzed subset based feature selection methods which have not been used previously for the purpose of phishing websites detection based on URL.

REFERNCES:

1. URL-based Phishing Websites Detection via Machine Learning | IEEE Conference Publication | IEEE Xplore

2. A Machine Learning Approach for URL Based Web Phishing Using Fuzzy Logic as Classifier | IEEE Conference Publication | IEEE Xplore

3.IEEE Xplore - Conference Table of Contents

4.A Methodical Overview on Detection, Identification and Proactive Prevention of Phishing Websites | IEEE Conference Publication | IEEE Xplore

5. Feature extraction and classification phishing websites based on URL | IEEE Conference Publication | IEEE Xplore